File 348:EUROPEAN PATENTS 1978-2004/Feb W03
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040219,UT=20040212
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	30847	LATTICE? ? OR LATICE? ?
S2	438140	BASES OR BASIS
S3	10136	S2(5N)(LONG??? OR LARGE??)
S4	6612	S2(5N)(SMALL??? OR SHORT???)
S5	49851	(DIGITAL? OR ELECTRONIC?)(3N)(SIGN OR SIGNS OR SIGNED OR SIGNING OR SIGNER OR SIGNATURE? ?)
S6	6345	PUBLIC()KEY? ? OR (ASYMMETRIC? OR TWO(W)KEY? ?)(3N)(CRYPT? OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD? OR SCRAMBL?)
S7	42220	CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR UNENCRYPT? OR UNSCRAMBL?
S8	2157	(AUXILIARY OR ALTERNATE OR ALTERNATIVE OR ANOTHER OR OTHER OR SEPARATE OR SECOND? OR 2ND OR ADDITIONAL)(5W)S1
S9	48	S2(50N)S8
S10	1	S3(50N)S8
S11	0	S4(50N)S8
S12	2	S5(50N)S8
S13	1	S6(50N)S8
S14	1	S7(50N)S8
S15	52	S9:S14

15/3,K/31 (Item 31 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00245318
Decoding of lattices and codes.
Dekodierung von Bruckennetzwerken und Koden.
Decodage de montages en pont et de codes.
PATENT ASSIGNEE:
CODEX CORPORATION, (604591), Moresfield Farm 7 Blue Hill River Road, Canton Massachusetts 02021, (US), (applicant designated states: BE;DE;FR;GB;IT;NL;SE)
INVENTOR:
Forney, George D., Jr., Six Coolidge Hill Road, Cambridge Massachusetts 02138, (US)
LEGAL REPRESENTATIVE:
Deans, Michael John Percy (30021), Lloyd Wise, Tregear & CO. Norman House 105-109 Strand, London WC2R OAE, (GB)
PATENT (CC, No, Kind, Date): EP 237186 A2 870916 (Basic)
EP 237186 A3 890322
EP 237186 B1 930421
APPLICATION (CC, No, Date): EP 87301139 870210;
PRIORITY (CC, No, Date): US 828397 860211
DESIGNATED STATES: BE; DE; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS: H03M-013/00; H03M-013/12; H04L-027/02;
ABSTRACT WORD COUNT: 268

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	3930
CLAIMS B	(German)	EPBBF1	2386
CLAIMS B	(French)	EPBBF1	2667
SPEC B	(English)	EPBBF1	16468
Total word count - document A			0
Total word count - document B			25451
Total word count - documents A + B			25451

...SPECIFICATION each of the two said parts, and means for selecting as a survivor from each of said multiple sets one said partial codeword on the **basis** of said distances, and for providing information indicative of each of said multiple survivors and its distance to subsequent said decoding substages of said **second** stage, or, **if** said substage **is** the final said substage, as a final output of said decoder.
Such trellis-type decoding of lattices and codes is loss complex than known decoding...
...a band-limited channel is encoded into a succession of codewords, and wherein the decoder comprises means for deciding which codeword was sent on the **basis** of a received set of values corresponding to the N-tuple r. In the case of **lattice** decoding, the **lattice** is equivalent to a 24-dimensional Leech-type lattice whose points have integer coordinates, and the maximum number of survivors in any substage is 2...

15/3,K/35 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01047182 **Image available**
TEXT MESSAGE GENERATION
GENERATION DE MESSAGES TEXTE
Patent Applicant/Assignee:
PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH, Steindamm 94, 20099 Hamburg, DE, DE (Residence), DE (Nationality), (Designated only for: DE)
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality), (For all designated states except: DE US)

Patent Applicant/Inventor:
PANKERT Matthias, c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen, DE, DE (Residence), BE (Nationality), (Designated only for: US)
SCHMALD Reimund, c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen, DE, DE (Residence), DE (Nationality), (Designated only for: US)
MARSCHNER Jens Friedemann, c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen, DE, DE (Residence), DE (Nationality), (Designated only for: US)
Legal Representative:
VOLMER Georg (agent), Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen, DE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200377234 A1 20030918 (WO 0377234)
Application: WO 2003IB890 20030310 (PCT/WO IB0300890)
Priority Application: DE 10211777 20020314
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 3552

Fulltext Availability:
Detailed Description
Detailed Description
... if the generated recognition result is satisfactory. If the grammar-based processing in block 804 does not produce a satisfactory result, the best word sequence **alternative** derivable from the word **lattice** generated by the ngram speech recognition device 803 is defined as recognition result, i.e. as text message, in a post-processing unit represented by a block 805 on the **basis** of said word lattice and is forwarded to the output unit 208, which outputs the generated text message to the respective addressees.

CLAWS.

1. A...

15/3,K/36 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01021050 **Image available**
DIGITAL SIGNATURE AND AUTHENTICATION METHOD AND APPARATUS
SIGNATURE NUMERIQUE ET PROCEDE ET DISPOSITIF D'AUTHENTIFICATION
Patent Applicant/Assignee:
NTRU CRYPTOSYSTEMS INC, 5 Burlington Woods, Burlington, MA 01803, US, US (Residence), US (Nationality)
Inventor(s):
HOFFSTEIN Jeffrey, 3 Leicester Way, Pawtucket, RI 02860, US,
HOWGRAVE-GRAHAM Nicholas A, 30 Park Street, Arlington, MA 02474, US,
PIPHER Jill C, 3 Leicester Way, Pawtucket, RI 02860, US,
SILVERMAN Joseph H, 57 North Hill Avenue, Needham, MA 02492, US,
WHYTE William J, 20 Bay State Road, Somerville, MA 02144, US,
Legal Representative:
BEVILACQUA Michael J (et al) (agent), Hale and Dorr LLP, 60 State Street, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200350998 A1 20030619 (WO 0350998)

Application: WO 2002US38640 20021206 (PCT/WO US0238640)
Priority Application: US 2001338330 20011207
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 16591

Fulltext Availability:
Detailed Description

Detailed Description
... and its rotations are probably the shortest such vectors. With the parameter choice (12), this problem is identical to the problem of breaking an NTRuENCRYlyr **public key** with the same parameters. Experiments give an estimated breaking time greater than 1012 MIPS years for the parameters (1 2).

Another way to use **lattice** reduction is to try to directly locate a valid signature (s,t). This problem is clearly an approximate closest vector problem (appr-CVP), since the...

39/5/1 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

08541518 Genuine Article#: 298NW Number of References: 62
Title: A progress report on lattice based public - key cryptosystems - Theoretical security versus practical cryptanalysis
Author(s): Sakurai K (REPRINT)
Corporate Source: KYUSHU UNIV,DEPT COMP SCI/FUKUOKA 8128581//JAPAN/ (REPRINT)
Journal: IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, 2000, VE83D, N3 (MAR), P570-579
ISSN: 0916-8532 Publication date: 20000300
Publisher: IEICE-INST ELECTRONICS INFORMATION COMMUNICATIONS ENG, KIKAI-SHINKO-KAIKAN BLDG MINATO-KU SHIBAKOEN 3 CHOME, TOKYO 105, JAPAN
Language: English Document Type: ARTICLE
Geographic Location: JAPAN
Subfile: CC ENGI--Current Contents, Engineering, Computing & Technology
Journal Subject Category: COMPUTER SCIENCE, INFORMATION SYSTEMS; COMPUTER SCIENCE, SOFTWARE, GRAPHICS, PROGRAMMING
Abstract: We review **public - key** cryptosystems from **lattice** problems, which are inspired by **Ajtai** 's remarkable result, and consider their security from the point of view of both theory and practice. We also survey recent results on the power of the **lattice** reduction algorithm in cryptanalysis.
Descriptors--Author Keywords: **public - key** cryptosystems ; **lattice** reduction problems ; LLL-algorithm ; cryptanalysis
Identifiers--KeyWord Plus(R): **BASIS** REDUCTION ALGORITHMS; APPROXIMATE OPTIMA; LINEAR-EQUATIONS; HARDNESS; SYSTEMS; CODES
Cited References:
ADLEMAN L, 1995, UNPUB FACTORING LATT
ADLEMAN L, 1983, P402, 15TH P ACM S THEOR C
AJTAI M, 1997, EL C COMP COMPL
AJTAI M, 1996, EL C COMP COMPL ECCC
AJTAI M, 1996, P 28 ANN ACM S THEOR
AJTAI M, 1998, P 30 ACM S THEOR COM
AJTAI M, 1997, TR97047 ECCC
ARORA S, 1997, V54, P317, J COMPUT SYST SCI
ARORA S, 1993, P724, 34TH P AN S FDN COMP
BABAI L, 1986, V6, P1, COMBINATORICA
BOAS PV, 1981, 8104 TR U AMST MATH
BONEH D, 1996, V1109, P129, LECT NOTES COMPUTER
BONEH D, 1999, V1592, P1, LECT NOTES COMPUTER
BONEH D, P CRYPT 99
BRICKELL E, 1985, V196, P342, LECT NOTES COMPUTER
BRICKELL EF, 1992, P501, CONT CRYPTOLOGY SCI
CAI J, IN PRESS TCS
CAI J, 1998, V1556, P219, LECT NOTES COMPUTER
CAI JY, IN PRESS THEORETICAL
CAI JY, 1999, P158, P 14 IEEE C COMP COM
CAI JY, 1997, UNPUB APPROXIMATING
CASSELS JWS, 1959, INTRO GEOMETRY NUMBE
CHEE YM, 1991, P CRYPT 91
COHEN H, V138, SPRINGER GTM
COPPERSMITH D, 1997, V10, P233, J CRYPTOL
COPPERSMITH D, 1997, V1233, P52, LECT NOTES COMPUTER
[illegible]STER MJ, 1992, V2, P111, COMPUT COMPLEX
[illegible]GLE C, 1999, LECT NOTES COMPUTER
LENSTRA BMM, 1987, V26, P325, J NUMBER THEORY
MIMUR I, P99, P FOCS98
DYER M, 1991, V38, P1, J ASSOC COMPUT MACH
FRIEZE AM, 1988, V17, P262, SIAM J COMPUT
GAUSS CF, 1801, DISQUISITIONES ARITH
GOLDREICH O, EL C COMP COMPL
GOLDREICH O, V1294, P105, LECT NOTES COMPUTER
GOLDREICH O, V1294, P112, LECT NOTES COMPUTER
GROTSCHEL M, 1988, GEOMETRIC ALGORITHMS
GRUBER PM, 1987, GEOMETRY NUMBERS

LAGARIAS J, 1983, P1, 24TH P AN S FDN COMP
LOVASZ L, 1986, ALGORITHMIC THEORY N
MERKLE RC, 1978, V24, P525, IEEE T INFORM THEORY
MICCIANCIO D, 1998, MITLCSTM574
MINKOWSKI H, 1910, GEOMETRIE ZAHLEN
MISARSKY JF, 1997, P221, P CRYPT 97
NGUYEN P, EL C COMP COMPL
NGUYEN P, 1997, V1294, P198, LECT NOTES COMPUTER
NGUYEN P, 1998, LECT NOTES COMPUTER
NGUYEN P, 1998, V1423, LECT NOTES COMPUTER
NGUYEN P, 1998, V1462, P223, LECT NOTES COMPUTER
NGUYEN P, 1998, V1514, LECT NOTES COMPUTER
NGUYEN P, P CRYPT 99
RITTER H, 1997, FACTORING VIA STRONG
SCHNORR CP, 1993, V13, P171, AMS DIMACS SERIES DI
SCHNORR CP, 1988, V9, P47, J ALGORITHM
SCHNORR CP, 1995, V921, P1, LECT NOTES COMPUTER
SCHNORR CP, 1994, V66, P181, MATH PROGRAM
SCHNORR CP, 1987, V53, P201, THEOR COMPUT SCI
SHAMIR A, 1982, P145, P 23 IEEE S FDN COMP
SHOUP V, NUMBER THEORY C PLUS
SMART NP, 1998, V41, LONDON MATH SOC STUD
STERN J, 1990, P313, P EUR 90
STERN J, 1987, P421, 28TH P AN S FDN COMP

39/5/2 (Item 1 from file: 239)

03060262 MR 2000i#94002

Cryptography.

Dedicated to Prof. Arto Salomaa on the occasion of his 65th birthday. Edited by C. Ding. Theoret. Comput. Sci. 226 (1999), no. 1-2.

Contributors: Ding, C.; Salomaa, Arto
Publ: Elsevier Science Publishers, B.V., Amsterdam, 1999, pp. ix--xii and 1--223. ISSN: 0304-3975 CODEN: TCSDI
Language: English
Document Type: Book; Proceedings
Journal Announcement: 200003
Cryptography; Special Issue: Cryptography; Festschrift: Salomaa, Arto K.; Birthday: Salomaa, Arto K.
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (28 lines)

Contents: Juhani Karhumaki, A short biography of Arto Salomaa (2--5); Leonard M. Adleman, Jonathan DeMarrais and Ming-Deh Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over ${\rm GF}(q)$ (7--18); Seng Kiat Chua, Ka Hin Leung and San Ling, Attack on RSA-type cryptosystems based on singular cubic curves over $\bold Z$ (19--27); Thomas W. Cusick, The **Ajtai** random class of **lattices** (29--36); Dengguo Feng, Three characterizations of [illegible]-immune functions over rings $Z\sb N$ (37--43); Dieter [illegible], Dual **bases** and bit-serial multiplication in $\bold F\sb {q\sp n}$ (45--59); Andrew Klapper and Jinzhong Xu, Algebraic feedback shift registers (61--92); Harald Niederreiter and Michael Vielhaber, An algorithm for shifted continued fraction expansions in parallel linear time (93--104); Valtteri Niemi and Ari Renvall, Efficient voting with no selling of votes (105--116); Joseph O Ruanaidh, Holger Petersen, Alexander Herrigel, Shelby Pereira and Thierry Pun, Cryptographic copyright protection for digital images based on watermarking techniques (117--142); Renji Tao and Shihua Chen [Shi Hua Chen 1], On finite automaton **public** - **key** cryptosystem (143--172); Vijay Varadharajan, Khanh Quoc Nguyen and Yi Mu, On the design of efficient RSA-based off-line electronic cash schemes (173--184); Chunru Zhang, Kwok-Yan Lam and Sushil Jajodia, Scalable threshold closure (185--206); Yuliang Zheng, Xian-Mo Zhang and Hideki Imai, Restriction, terms and nonlinearity of Boolean functions (207--223).

\{Most of the papers are being reviewed individually.\}

Reviewer: Editors

Review Type: Table of contents
Descriptors: *94-06 -Information and communication, circuits-Proceedings, conferences, collections, etc. ; 00B30 -General-Conference proceedings and collections of papers-Festschriften

39/5/3 **(Item 2 from file: 239)**
DIALOG(R)File 239:Mathsci

02953741 MR 99k#94034
Positive applications of lattices **to cryptography.**
Mathematical foundations of computer science 1997 (Bratislava)
Dwork, Cynthia (IBM Research Division, San Jose, California, 95120
Corporate Source Codes: 1-IBM2
1997,
Springer, Berlin,; 44--51,,
Series: Lecture Notes in Comput. Sci., 1295,
Language: English Summary Language: English
Document Type: Proceedings Paper
Journal Announcement: 9817
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (17 lines)
Introduction: ``Initiated by M. **Ajtai** 's paper [in Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996), 99--108, ACM, New York, 1996; see MR 97g:68005 \refcno 1427503\endrefcno], a burgeoning effort to build cryptographic primitives based on the assumed hardness of worst-case or random instances of problems involving **lattices** has proved extremely fruitful. Prior to **Ajtai** 's work, **lattices** , and in particular, the **lattice basis** reduction algorithm of Lenstra, Lenstra and Lovasz, were used in cryptography principally to prove cryptographic insecurity. We describe more positive applications of **lattices** : constructions for **public key** cryptosystems, cryptographically strong hash functions, pseudo-random bit generators whose security depends only on the worst-case hardness of the underlying **lattice** problem and a digital signature scheme whose security depends on the average hardness of the underlying problem.''

35/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7121493 INSPEC Abstract Number: B2002-01-6120D-115, C2002-01-1260C-090
Title: The two faces of lattices in cryptology
Author(s): Nguyen, P.Q.; Stern, J.
Author Affiliation: Dept. d'Inf., Ecole Normale Superieure, Paris, France
Conference Title: Cryptography and Lattices. International Conference, CaLC 2001. Revised Papers (Lecture Notes in Computer Science Vol.2146) p.146-80
Editor(s): Silverman, J.H.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 2001 Country of Publication: Germany vi+217 pp.
ISBN: 3 540 42488 1 Material Identity Number: XX-2001-02453
Conference Title: Cryptography and Lattices. International Conference, CALC 2001. Revised Papers
Conference Sponsor: NTRU Cryptosyst
Conference Date: 29-30 March 2001 Conference Location: Providence, RI, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Bibliography (B); Theoretical (T)
Abstract: **Lattices** are regular arrangements of points in n-dimensional space, whose study appeared in the nineteenth century in both number theory and crystallography. Since the appearance of the celebrated Lenstra-Lenstra-Lovasz **lattice basis** reduction algorithm twenty years ago, **lattices** have had surprising applications in cryptology. Until recently, the applications of **lattices** to cryptology were only negative, as **lattices** were used to break various cryptographic schemes. Paradoxically, several positive cryptographic applications of **lattices** have emerged in the past five years: there now exist **public - key** cryptosystems based on the hardness of **lattice** problems, and **lattices** play a crucial role in a few security proofs. We survey the main examples of the **two** faces of **lattices** in cryptology. (137 Refs)
Subfile: B C
Descriptors: **lattice** theory; number theory; **public key** cryptography
Identifiers: **lattices** ; cryptology; number theory; Lenstra-Lenstra-Lovasz **lattice basis** reduction algorithm; **public - key** cryptosystems; problem hardness; security proofs
Class Codes: B6120D (Cryptography); B0250 (Combinatorial mathematics); C1260C (Cryptography theory); C1160 (Combinatorial mathematics)

35/5/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6381279 INSPEC Abstract Number: C1999-11-1260C-052
Title: The Ajtai random class of lattices
Author(s): Cusick, T.W.
Author Affiliation: Dept. of Math., State Univ. of New York, Buffalo, NY, USA
Journal: Theoretical Computer Science vol.226, no.1-2 p.29-36
Publisher: Elsevier,
Publication Date: 17 Sept. 1999 Country of Publication: Netherlands
CODEN: TCSCDI ISSN: 0304-3975
SICI: 0304-3975(19990917)226:1/2L.29:ARCL;1-9
Material Identity Number: T168-1999-018
U.S. Copyright Clearance Center Code: 0304-3975/99/$20.00
Document Number: S0304-3975(99)00063-8
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: Ajtai has recently given a reduction from the problem of approximating a **short basis** for a **lattice** in the worst case, to the problem of finding a short **lattice** vector for a uniformly chosen **lattice** in a certain random class of **lattices** . Here we give an explicit formula for the number of **lattices** of the type used by Ajtai. We also prove some

results about the average volume of the fundamental cell of such a **lattice** . (4 Refs)
Subfile: C
Descriptors: **public key** cryptography
Identifiers: random class of **lattices** ; cryptography; Ajtai random class ; **lattice** ; provably secure cryptosystem
Class Codes: C1260C (Cryptography theory)

35/5/3 **(Item 1 from file: 144)**
DIALOG(R)File 144:Pascal

14254193 PASCAL No.: 99-0457361
Generating hard instances of the short basis **problem**
Automata, languages and programming : Prague, 11-15 July 1999
AJTAI M
WIEDERMANN Jiri, ed; VAN EMDE BOAS Peter, ed; NIELSEN Mogens, ed
IBM Almaden Research Center, CA 95120, United States
ICALP '99 :international colloquium on automata, languages and programming, 26 (Prague CZE) 1999-07-11
Journal: Lecture notes in computer science, 1999, 1644 1-9
ISBN: 3-540-66224-3 ISSN: 0302-9743 Availability: INIST-16343;
[illegible]
[illegible] Refs.: 7 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
A class of random **lattices** is given, in (1) so that (a) a random **lattice** can be generated in polynomial time together with a short vector in it, and (b) assuming that certain worst-case **lattice** problems have no polynomial time solutions, there is no polynomial time algorithm which finds a short vector in a random **lattice** with a polynomially large probability. In this paper we show that **lattices** of the same random class can be generated not only together with a short vector in them, but also together with a **short basis** . The existence of a known **short basis** may make the construction more applicable for cryptographic protocols.

English Descriptors: Computer theory; Computational complexity; Algorithm complexity; **Public key** cryptography; Security of data; Computer security

French Descriptors: Informatique theorique; Complexite calcul; Complexite algorithme; Cryptographie cle publique; Securite donnee; Securite informatique

Classification Codes: 001D02A05; 001D04A04E

35/5/4 **(Item 1 from file: 239)**
DIALOG(R)File 239:Mathsci

03154747 MR 2001f#68008
Automata, languages and programming.
Proceedings of the 27th International Colloquium (ICALP 2000) held at the University of Geneva, Geneva, July 9--15, 2000. Edited by Ugo Montanari, Jose D. P. Rolim and Emo Welzl.
Contributors: Montanari, Ugo; Rolim, Jose D. P.; Welzl, Emo
Publ: Springer-Verlag, Berlin,
2000, xvi+941 pp. ISBN: 3-540-67715-1
Series: Lecture Notes in Computer Science, 1853.
Price: \$89.00.
Language: English

Document Type: Book; Proceedings
Journal Announcement: 200104
Automata, languages and programming; Colloquium: Automata, Languages and Programming,; Geneva,; Lecture Notes in Computer Science, 27th International, ICALP 2000 2000 1853
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (150 lines)
The 26th Colloquium has been reviewed [MR 2000j:68001].\}

Contents: Samson Abramsky, Game semantics: achievements and prospects (1); Lars Engebretsen and Jonas Holmerin, Clique is hard to approximate within $n\sp {1-o(1)}$ (2--12); Michael Krivelevich and Van H. Vu, Approximating the independence number and the chromatic number in expected polynomial time (13--24); Cristiano Calcagno, Eugenio Moggi and Walid Taha, Closed types as a simple approach to safe imperative multi-stage programming (25--36); Alan Mycroft and Richard Sharp, A statically allocated parallel functional language (37--48); Seth Pettie and Vijaya Ramachandran, An optimal minimum spanning tree algorithm (49--60); Torben Hagerup, Improved shortest paths on the word RAM (61--72); Stephen Alstrup and Jacob Holm, Improved algorithms for finding level ancestors in dynamic trees (73--84); Gordon Plotkin and John Power [A. John Power], Lax logical relations (85--102); Dan R. Ghica and Guy McCusker, Reasoning about Idealized ALGOL using regular languages (103--115).

Keye Martin, The measurement process in domain theory (116--126); Gregor Engels and Reiko Heckel, Graph transformation as a conceptual and formal framework for system modeling and model evolution (127--150); Albert Atserias, Nicola Galesi and Ricard Gavalda, Monotone proofs of the pigeon hole principle (151--162); Gerald Luttgen and Michael Mendler, Fully-abstract statecharts semantics via intuitionistic Kripke models (163--174); Roberto Bruni and Vladimiro Sassone, Algebraic models for contextual nets (175--186); Beate Bollig and Ingo Wegener, Asymptotically optimal bounds for OBDDs and the solution of some basic OBDD problems (extended abstract) (187--198); Juraj Hromkovic, Juhani Karhumaki, Hartmut Klauck, Georg Schnitger and Sebastian Seibert, Measures of nondeterminism in finite automata (199--210); Volker Diekert and Paul Gastin, LTL is expressively complete for Mazurkiewicz traces (211--222); Ben C. Moszkowski, An automata-theoretic completeness proof for interval temporal logic (extended abstract) (223--234); J. Hastad, Which NP-hard optimization problems admit non-trivial efficient approximation algorithms? (235).

Evgeny Dantsin [E. Ya. Dantsin], Andreas Goerdt, Edward A. Hirsch and Uwe Schoning, Deterministic algorithms for k-SAT based on covering codes and local search (236--247); Johannes Blomer, Closest vectors, successive minima, and **dual** HKZ- **bases** of **lattices** (248--259); Leonid Libkin, Variable independence, quantifier elimination, and constraint representations (260--271); Andrei A. Bulatov, Andrei A. Krokhin and Peter Jeavons, Constraint satisfaction problems and finite algebras (272--282); Steven S. Seiden, An optimal online algorithm for bounded space variable-sized bin packing (283--295); Janos Csirik and Gerhard J. Woeginger, Resource augmentation for online bounded space bin packing (extended abstract) (296--304); Christoph Ambuhl, Bernd Gartner and Bernhard von Stengel, Optimal projective algorithms for the list update problem (305--316); Antonin Kucera, Efficient verification algorithms for one-counter processes (317--328); Richard Mayr, On the complexity of bisimulation problems for basic parallel processes (329--341); Denis Lugiez and Philippe Schnoebelen, Decidable first-order transition logics for PA-processes (342--353).

Riccardo Focardi, Roberto Gorrieri and Fabio Martinelli, Non-interference for the analysis of cryptographic protocols (354--372); Ali Akhavi and Brigitte Vallee, Average bit-complexity of Euclidean algorithms (373--387); Cyril Banderier, Philippe Flajolet, Gilles Schaeffer and Michele Soria, Planar maps and Airy phenomena (388--402); Barbara Konig, Analysing input/output-capabilities of mobile processes with a generic type system (403--414); Matthew Hennessy and James Riely, Information flow vs. resource access in the asynchronous pi-calculus (extended abstract) (415--427); Richard M. Karp, The genomics revolution and its challenges for algorithmic research (428); Zohar Manna and Henny B. Sipma, Alternating the temporal picture for safety (429--450); Alfredo De Santis, Giovanni Di Crescenzo and Giuseppe Persiano, Necessary and

sufficient assumptions for non-interactive zero-knowledge proofs of knowledge for all NP relations (extended abstract) (451--462); William Aiello, Sandeep Bhatt, Rafail Ostrovsky and S. Raj. Rajagopalan, Fast verification of any remote procedure call: short witness-indistinguishable [illegible] proofs for NP (463--474); Javier Esparza and Keijo Heljanko, A new unfolding approach to LTL model checking (475--486).

S. Meenakshi and R. Ramanujam, Reasoning about message passing in finite state environments (487--498); Olivier Baudron, David Pointcheval and Jacques Stern, Extended notions of security for multicast **public key** cryptosystems (499--511); Christian Cachin, Jan Camenisch, Joe Kilian and Joy Muller, One-round secure computation and secure autonomous mobile agents (extended abstract) (512--523); Birgit Baum-Waidner and Michael Waidner, Round-optimal and abuse-free optimistic multi-party contract signing (524--535); Juhani Karhumaki and Ion Petre, On the centralizer of a finite set (536--546); Frank Neven and Thomas Schwentick, On the power of tree-walking automata (547--560); Marie-Pierre Beal and Olivier Carton, Determinization of transducers over infinite words (561--570); Kurt Mehlhorn, Constraint programming and graph algorithms (571--575); Noga Alon, Haim Kaplan, Michael Krivelevich, Dahlia Malkhi and Julien Stern, Scalable secure storage when half the system is faulty (576--587); Endre Boros, Vladimir Gurvich, Leonid Khachiyan and Kazuhisa Makino, Generating partial and multiple transversals of a hypergraph (588--599).

Jose Espirito Santo, Revisiting the correspondence between cut elimination and normalisation (600--611); Reinhard Pichler, Negation elimination from simple equational formulae (612--623); V. S. Anil Kumar, Sunil Arya and H. Ramesh, Hardness of set cover with intersection 1 (624--635); Michael Elkin and David Peleg, Strong inapproximability of the basic k-spanner problem (extended abstract) (636--647); Dietrich Kuske, Infinite series-parallel posets: logic and languages (648--662); Tomasz Fryderyk Urbanski, On deciding if deterministic Rabin language is in Buchi class (663--674); Jesper G. Henriksen, Madhavan Mukund, K. Narayan Kumar and P. S. Thiagarajan, On message sequence graphs and finitely generated regular MSC languages (675--686); Oded Goldreich, Pseudorandomness (687--704); Leslie Ann Goldberg, Mark Jerrum, Sampath Kannan and Mike Paterson, A bound on the capacity of backoff and acknowledgement-based protocols (705--716); Bogdan S. Chlebus, Leszek Gasieniec, Anna Ostlin and John Michael Robson, Deterministic radio broadcasting (717--728).

W. J. Fokkink and S. P. Luttik, An ω-complete equational specification of interleaving (extended abstract) (729--743); Mario Bravetti and Roberto Gorrieri, A complete axiomatization for observational congruence of prioritized finite-state behaviors (744--755); Micah Adler, Faith Fich, Leslie Ann Goldberg and Mike Paterson, Tight size bounds for packet headers in narrow meshes (756--767); Luciano Margara and Janos Simon, Wavelength assignment problem on all-optical networks with k fibres per link (768--779); Christel Baier, Boudewijn Haverkort, Holger Hermanns and Joost-Pieter Katoen, On the logical characterisation of performability properties (780--792); Olivier Bournez and Oded Maler, On the representation of timed polyhedra (793--807); Andrei Z. Broder, Min-wise independent permutations: theory and practice (808); Michael A. Bender and Dana Ron, Testing acyclicity of directed graphs in sublinear time (809--820); Hristo N. Djidjev, Computing the girth of a planar graph (821--831); Herve Fournier and Pascal Koiran, Lower bounds are not easier over the reals: inside PH (832--843).

Ganesh Baliga, John Case, Wolfgang Merkle and Frank Stephan, Unlearning helps (844--855); Artur Czumaj and Andrzej Lingas, Fast approximation schemes for Euclidean multi-connectivity problems (extended abstract) (856--868); Michelangelo Grigni, Approximate TSP in graphs with forbidden minors (869--877); Klaus Jansen and Lorant Porkolab, Polynomial time approximation schemes for general multiprocessor job shop scheduling (878--889); Pierre McKenzie, Thomas Schwentick, Denis Therien and Heribert Vollmer, The many faces of a translation (890--901); Jack H. Lutz, Gales and the constructive dimension of individual sequences (902--913); Wolfgang Merkle, The global power of additional queries to p-random oracles (914--925); Josh Buresh-Oppenheim, Toniann Pitassi, Matt Clegg and Russell Impagliazzo, Homogenization and the polynomial calculus (926--937).

\{Most of the papers are being reviewed individually.\}

Reviewer: Editors

Review Type: Table of contents

Descriptors: '68-06 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Proceedings, conferences, collections, etc.

35/5/5 (Item 2 from file: 239)
DIALOG(R)File 239:Mathsci

02285211 MR 92h#94020
Insecurity of the knapsack one-time pad.
Number theory and cryptography (Sydney, 1989)
Worley, R. T. (Department of Mathematics, Monash University, Clayton, VIC 3168, Australia)
Corporate Source Codes: 5-MNSH
1990,
Cambridge Univ. Press, Cambridge,; 156--164,,
Series: London Math. Soc. Lecture Note Ser., 154,
Language: English
Document Type: Proceedings Paper
Journal Announcement: 9013
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (15 lines)
Introduction: `` **Public key** cryptosystems based on the knapsack trapdoor have been considered insecure since a polynomial time algorithm was found for breaking instances of the code. In particular, the Lenstra, Lenstra and Lovasz algorithm for producing **short basis** vectors of a **lattice** has proved useful in attacking the Diophantine approximation problems which arise in attempts to break the codes. L. O'Connor [``An approximation to the one-time pad'', Rep. No. 328, Dept. Comput. Sci., Univ. Sydney, Sydney, 1988; per bibl.] has proposed an interesting variant of the knapsack cryptosystem. Unfortunately, as will be shown, the Diophantine equations associated with the system fall to the **short basis** vector attack. All instances of the proposed system that have been generated to test the system have been broken. It seems that there are many sets of parameters that will generate any instance of the code, and it is too easy to find such a set.''

25/5/9 (Item 1 from file: 65)
DIALOG(R)File 65:Inside Conferences

04516474 INSIDE CONFERENCE ITEM ID: CN047232351
Fast- lattice -based polynomial digital signature system for m-commerce (4793-06)
Wei, X.; Leung, L.; Anshel, M.
CONFERENCE: Mathematics of data/image coding, compression and encryption V with applications-Conference
PROCEEDINGS-SPIE THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING, 2003 ; VOL 4793 P: 52-56
SPIE, 2003
ISSN: 0277-786X ISBN: 0819445606
LANGUAGE: English DOCUMENT TYPE: Conference Papers
CONFERENCE EDITOR(S): Schmalz, M. S.
CONFERENCE SPONSOR: International Society for Optical Engineering
CONFERENCE LOCATION: Seattle, WA 2002; Jul (200207) (200207)

BRITISH LIBRARY ITEM LOCATION: 6823.100000
DESCRIPTORS: mathematics; SPIE; encryption V; data coding; image coding

25/5/12 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

7659122 INSPEC Abstract Number: B2003-07-0100-055, C2003-07-0000-025
Title: Topics in Cryptology - CT-RSA 2003. Cryptoghraphers' Track at the RSA Conference 2003. Proceedings (Lecture Notes in Computer Science Vol.2612)
Editor(s): Joyce, M.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 2003 Country of Publication: Germany xi+416 pp.
ISBN: 3 540 00847 0 Material Identity Number: XX-2003-01257
Conference Title: Topics in Cryptology - CT-RSA 2003. Cryptographers' Track at the RSA Conference 2002. Proceedings
Conference Date: 13-17 April 2003 Conference Location: San Francisco, CA, USA
Language: English Document Type: Conference Proceedings (CP)
Abstract: The following topics are dealt with: key self-protection; message authentication; **digital signatures** ; pairing based cryptography; multivariate and **lattice** problems; cryptographic architectures; RSA-based cryptosystems; chosen-ciphertext security; broadcast encryption and PRF sharing; authentication structures; elliptic curves and pairings; threshold cryptography; implementation issues.
Subfile: B C
Descriptors: cryptography; Galois fields; message authentication
Identifiers: cryptology; key self-protection; message authentication; **digital signatures** ; pairing based cryptography; multivariate problems; **lattice** problems; cryptographic architectures; RSA-based cryptosystems; chosen-ciphertext security; broadcast encryption; PRF sharing; authentication structures; elliptic curves; threshold cryptography; implementation issues
Class Codes: B0100 (General electrical engineering topics); B6120D (Cryptography); C0000 (General and management topics); C1260C (Cryptography theory); C6130S (Data security)

25/5/13 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

7393161 INSPEC Abstract Number: B2002-11-6120D-005, C2002-11-1260C-005
Title: On the security of the digital signature algorithm
Author(s): Blake, I.F.
Author Affiliation: Dept. of Electr. & Comput. Eng., Toronto Univ., Ont.,

Canada
Journal: Designs, Codes and Cryptography vol.26, no.1-3 p.87-96
Publisher: Kluwer Academic Publishers,
Publication Date: June-Aug. 2002 Country of Publication: Netherlands
CODEN: DCCREC ISSN: 0925-1022
SICI: 0925-1022(200206/08)26:1/3L.87:SDSA;1-R
Material Identity Number: O660-2002-004
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: We present a key-recovery attack against the **digital signature** algorithm (DSA). Our method is based on the work of Coppersmith (1997), and is similar in nature to the attacks of Boneh et al. (2000) which use **lattice** reduction techniques to determine upper bounds on the size of an RSA decryption exponent under which it will be revealed by the attack. This work similarly determines provable upper bounds on the sizes of the two key parameters in the DSA for which the system can be broken. Specifically if about half of the total number of bits in the secret and ephemeral keys, assuming contiguous unknown bits in each key, are known, the system can be shown to be insecure. The same technique shows that if about half of the total number of bits in two ephemeral keys are known, again assumed contiguous unknown bits in each key, but with no knowledge of the secret key, the system can be shown to be insecure. (20 Refs)
Subfile: B C
Descriptors: cryptography; **lattice** theory; message authentication
Identifiers: key-recovery attack; **digital signature** algorithm; cryptography; security; **lattice** reduction techniques; upper bounds; RSA decryption exponent; secret keys; ephemeral keys
Class Codes: B6120D (Cryptography); C1260C (Cryptography theory)

25/5/14 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

7121490 INSPEC Abstract Number: B2002-01-6120D-112, C2002-01-1260C-087
Title: The insecurity of Nyberg-Rueppel and other DSA-like signature schemes with partially known nonces
Author(s): El Mahassni, E.; Nguyen, P.Q.; Shparlinski, I.E.
Author Affiliation: Dept. of Comput., Macquarie Univ., North Ryde, NSW, Australia
Conference Title: Cryptography and Lattices. International Conference, CaLC 2001. Revised Papers (Lecture Notes in Computer Science Vol.2146) p.97-109
Editor(s): Silverman, J.H.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 2001 Country of Publication: Germany vi+217 pp.
ISBN: 3 540 42488 1 Material Identity Number: XX-2001-02453
Conference Title: Cryptography and Lattices. International Conference, CALC 2001. Revised Papers
Conference Sponsor: NTRU Cryptosyst
Conference Date: 29-30 March 2001 Conference Location: Providence, RI, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: It has been proved by Nguyen and Shparlinski (to appear) that the **digital signature** algorithm (DSA) is insecure when a few consecutive bits of the random nonces k are known for a reasonably small number of DSA signatures. This result confirmed the efficiency of some heuristic **lattice** attacks designed and numerically verified by Howgrave-Graham and Smart (to appear). Here we extend the attack to the Nyberg-Rueppel (1995) variants of DSA. We use a connection with the hidden number problem introduced by Boneh and Venkatesan and new bounds of exponential sums which might be of independent interest. (23 Refs)
Subfile: B C
Descriptors: cryptography; **lattice** theory; message authentication; number theory
Identifiers: insecurity; Nyberg-Rueppel variants; DSA; partially known

nonces; **digital signature** algorithm; heuristic **lattice** attacks; hidden number problem; exponential sum bounds
Class Codes: B6120D (Cryptography); B0250 (Combinatorial mathematics); C1260C (Cryptography theory); C1160 (Combinatorial mathematics)

25/5/16 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

6997359 INSPEC Abstract Number: B2001-09-6120D-022, C2001-09-1260C-020
Title: Lattice **attacks on** digital signature **schemes**
Author(s): Howgrave-Graham, N.A.; Smart, N.P.
Author Affiliation: IBM Thomas J. Watson Res. Center, Hawthorne, NY, USA
Journal: Designs, Codes and Cryptography vol.23, no.3 p.283-90
Publisher: Kluwer Academic Publishers,
Publication Date: Aug. 2001 Country of Publication: Netherlands
CODEN: DCCREC ISSN: 0925-1022
SICI: 0925-1022(200108)23:3L.283:LADS;1-Q
Material Identity Number: O660-2001-006
U.S. Copyright Clearance Center Code: 0925-1022/2001/$19.50
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T); Experimental (X)
Abstract: We describe a **lattice** attack on the **digital signature** algorithm (DSA) when used to sign many messages, m/sub i/, under the assumption that a proportion of the bits of each of the associated ephemeral keys, y/sub i/, can be recovered by alternative techniques. (11 Refs)
Subfile: B C
Descriptors: cryptography; message authentication
Identifiers: **digital signature** schemes; **lattice** attack; **digital signature** algorithm; associated ephemeral keys
Class Codes: B6120D (Cryptography); C1260C (Cryptography theory); C6130S (Data security)

25/5/19 (Item 10 from file: 2)
DIALOG(R)File 2:INSPEC

04169172 INSPEC Abstract Number: B9207-6140-165, C9207-5240-019
Title: **Efficient implementation of the normalized recursive least-square lattice filter**
Author(s): Sau-Gee Chen; Jin-Feng Lin
Author Affiliation: Dept. of Electron. Eng., Nat. Chiao Tung Univ., Hsinchu, Taiwan
Conference Title: ICASSP 91. 1991 International Conference on Acoustics, Speech and Signal Processing (Cat. No.91CH2977-7) p.1565-8 vol.3
Publisher: IEEE, New York, NY, USA
Publication Date: 1991 Country of Publication: USA 5 vol. 3732 pp.
ISBN: 0 7803 0003 3
U.S. Copyright Clearance Center Code: CH2977-7/91/0000-1565$01.00
Conference Sponsor: IEEE
Conference Date: 14-17 May 1991 Conference Location: Toronto, Ont., Canada
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: An efficient hardware implementation is proposed for the optimal, computationally intensive, normalized recursive least-squares **lattice** (NLSL) adaptive filter. NLSL operation steps are optimized for better hardware utilization. To best match the execution steps, a combined processing unit for radix-2 division and square-root operations, and a radix-4 MSB-first multiplication unit based on signed digit (SD) arithmetic are proposed. The proposed NLSL implementation achieves both good area and time performance. The approach is shown to be better than the CORDIC approach, and SD arithmetic is a good choice for implementing the

complicated signal processing algorithms. (11 Refs)
Subfile: B C
Descriptors: adaptive filters; digital arithmetic; digital filters; least squares approximations
Identifiers: **signed digital** arithmetic; optimised operation steps; normalized recursive least-square **lattice** filter; efficient hardware implementation; adaptive filter; combined processing unit; radix-2 division ; square-root operations; radix-4 MSB-first multiplication unit; signal processing algorithms
Class Codes: B6140 (Signal processing and detection); B0290F (Interpolation and function approximation); C5240 (Digital filters); C5230 (Digital arithmetic methods); C4130 (Interpolation and function approximation)

25/5/24 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04635742 JICST ACCESSION NUMBER: 00A0582104 FILE SEGMENT: JICST-E
Improvement of Phase Modulation Based Data Embedding Method for Still Pictures.
MINAMI NORIAKI (1); YAMADA YOSHIO (2); TAZAKI SABURO (3)
(1) Hiroshimakokusaigakuindai Gendaishakai; (2) Ehime Univ., Fac. of Eng. ; (3) Matsuyama Univ., Fac. of Econ.
Gazo Denshi Gakkaishi(Journal of the Institute of Image Electronics Engineers of Japan), 2000, VOL.29,NO.3, PAGE.214-221, FIG.11, REF.8
JOURNAL NUMBER: S0815AAG ISSN NO: 0285-9831
UNIVERSAL DECIMAL CLASSIFICATION: 681.3:621.397.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: Authors have already proposed a data embedding method based on the phase modulation of sampling **lattice** to picture coding. On this method, an original picture is necessary for decoding additional data as a standard reference information. In this paper, we positively utilize this feature and propose a new method in which we use a processed picture by data compression coding instead of the original picture as the standard reference information. We examine the proposed method with the authorized source coding (that is, JPEG). The results show that the new method can exactly improve error rate characteristic such that, for instance, as "Zelda", approximately 1,000 embedded data bits are decoded correctly with the JPEG compression ratio of 17 under the degradation of the signal-to-noise ratio within approximately 0.1 dB. (author abst.)
DESCRIPTORS: still-picture; JPEG; **digital signature** ; copyright; phase modulation; interposition; vector quantization; signal sampling; **lattice**
BROADER DESCRIPTORS: image; ISO Standard; international standard; standard(specification); standard; image compression; image processing; information processing; treatment; cryptogram; intellectual property; right; angle modulation; signal modulation; signal processing; insertion; signal quantization; quantization; modification
CLASSIFICATION CODE(S): JE04010I

25/5/26 (Item 3 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04613085 JICST ACCESSION NUMBER: 00A0001940 FILE SEGMENT: JICST-E
Data embedding method based on the phase modulation of sampling lattice . **Encoding process.**
MINAMI NORIAKI (1); YAMADA YOSHIO (1); TAZAKI SABURO (1); WAKASUGI KOICHIRO (2); KASAHARA MASAO (2)
(1) Ehime Univ., Fac. of Eng.; (2) Kyoto Inst. of Technol., Fac. of Eng. and Des.

Eizo Medea Shori Shinpojiumu Shiryo(Proceedings of the Ist Image Media Processing Symposium), 1998, VOL.3rd, PAGE.43-44, FIG.2, REF.2
JOURNAL NUMBER: L3261AAD
UNIVERSAL DECIMAL CLASSIFICATION: 681.3:621.397.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Conference Proceeding
ARTICLE TYPE: Short Communication
MEDIA TYPE: Printed Publication
DESCRIPTORS: image compression; **digital signature** ; phase modulation; signal sampling; **lattice** ; image coding; interposition; computer simulation
BROADER DESCRIPTORS: image processing; information processing; treatment; cryptogram; angle modulation; signal modulation; signal processing; modification; coding(signal); insertion; computer application; utilization; simulation
CLASSIFICATION CODE(S): JE04010I

25/5/31 (Item 3 from file: 144)
DIALOG(R)File 144:Pascal

16091655 PASCAL No.: 03-0248984
Enhancing simple power-analysis attacks on elliptic curve cryptosystems CHES 2002 : cryptographic hardware and embedded systems : Redwood Shores, 13-15 August 2002, revised papers
OSWALD Elisabeth
KALISKI Burton S, ed; KOC Cetin, ed; PAAR Christof, ed
Institute for Applied Information Processing and Communications, Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
Cryptographic hardware and embedded systems. International workshop, 4 (Redwood Shores CA USA) 2002-08-13
Journal: Lecture notes in computer science, 2002, 2523 82-97
ISBN: 3-540-00409-2 ISSN: 0302-9743 Availability: INIST-16343; 354000108498190070
No. of Refs.: 1 p.1/2
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
Recent applications of **lattice** attacks against elliptic curve cryptosystems have shown that the protection of ephemeral keys in the ECDSA is of greatest importance. This paper shows how to enhance simple power-analysis attacks on elliptic-curve point-multiplication algorithms by using Markov models. We demonstrate the attack on an addition-subtraction algorithm (fixing the sequence of elliptic-curve operations) which is similar to the one described by Morain et al. in (MO90) and apply the method to the general addition-subtraction method described in ANSI X9.62 (ANS99).

English Descriptors: Markov model; Cryptanalysis; Elliptic curve; **Digital signature** ; Randomised algorithms; Cryptosystem

French Descriptors: Modele Markov; Cryptanalyse; Courbe elliptique; Signature numerique; Algorithme randomise; Cryptosysteme

Classification Codes: 001D04A04E

25/5/46 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci

02805935 MR 98g#94023
Optimal tree-based one-time digital signature **schemes.**
STACS 96 (Grenoble, 1996)

Hirschenbacher, Daniel (Institut fur Theoretische Informatik, Eidgenossische TH Zurich-Zentrum, 8092 Zurich, Switzerland)
Maurer, Ueli M. (Institut fur Theoretische Informatik, Eidgenossische TH Zurich-Zentrum, 8092 Zurich, Switzerland)
Corporate Source Codes: CH-ETHZ-TI; CH-ETHZ-TI
1996,
Springer, Berlin,; 363--374,,
Series: Lecture Notes in Comput. Sci., 1046,
Language: English Summary Language: English
Document Type: Proceedings Paper
Journal Announcement: 9716
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (11 lines)
Summary: ``A minimal cutset of a tree directed from the leaves to the root is a minimal set of vertices such that every path from a leaf to the root meets at least one of these vertices. An order relation on the set of minimal cutsets can be defined: $U\le V$ if and only if every vertex of U is on the path from some vertex in V to the root. Motivated by the design of efficient cryptographic **digital signature** schemes, the problem of constructing trees with a large number of pairwise incomparable minimal cutsets or, equivalently, with a large antichain in the poset of minimal cutsets, is considered.''
\{For the entire collection see MR 98d:68022.\}
Reviewer: Summary
Review Type: Abstract
Proceedings Reference: 98d#68022; 1 462 080
Descriptors: *94A60 -Information and communication, circuits-Communication, information-Cryptography (See also 11T71, 68P25) ; 06A07 -Order, **lattices** , ordered algebraic structures (See also 18B35)-Ordered sets-Combinatorics of partially ordered sets; 68P25 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Theory of data-Data encryption (See also 94A60); 68R10 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Discrete mathematics in relation to computer science-Graph theory (See also 05Cxx, 90B10, 90B35, 90C35

21/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

5723753 INSPEC Abstract Number: C9711-6130S-080
Title: Positive applications of lattices to cryptography
Author(s): Dwork, G.
Author Affiliation: IBM Almaden Res. Center, San Jose, CA, USA
Conference Title: Mathematical Foundations of Computer Science 1997. 22nd International Symposium, MFCS'97 Proceedings p.44-51
Editor(s): Privara, I.; Ruzicka, P.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1997 Country of Publication: Germany x+517 pp.
ISBN: 3 540 63437 1 Material Identity Number: XX97-01900
Conference Title: Proceedings of 22nd International Symposium on Mathematical Foundations of Computer Science
Conference Date: 25-29 Aug. 1997 Conference Location: Bratislava, Slovakia
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We describe constructions of several cryptographic primitives, including hash functions, **public key** cryptosystems, pseudorandom bit generators, and **digital signatures** , whose security depends on the assumed worst-case or average-case hardness of problems involving **lattices** . (26 Refs)
Subfile: C
Descriptors: cryptography
Identifiers: cryptographic primitives; hash functions; **public key** cryptosystems; pseudorandom bit generators; **digital signatures** ; worst-case; average-case; hardness; **lattices**
Class Codes: C6130S (Data security)
Copyright 1997, IEE

21/5/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

5710023 INSPEC Abstract Number: B9711-6120B-051, C9711-6130S-031
Title: Public - key **cryptosystems from** lattice **reduction problems**
Author(s): Goldreich, O.; Goldwasser, S.; Halevi, S.
Author Affiliation: Weizmann Inst. of Sci., Rehovot, Israel
Conference Title: Advances in Cryptology - CRYPTO '97. 17th Annual International Cryptology Conference. Proceedings p.112-31
Editor(s): Kaliski, B.S., Jr.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1997 Country of Publication: Germany xii+537 pp.
ISBN: 3 540 63384 7 Material Identity Number: XX97-02096
Conference Title: Advances in Cryptology - CRYPTO'97. 17th Annual International Cryptology Conference. Proceedings
Conference Date: 17-21 Aug. 1997 Conference Location: Santa Barbara, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We present a new proposal for a trapdoor one-way function, from which we derive **public - key** encryption and **digital signatures** . The security of the new construction is based on the conjectured computational difficulty of **lattice** -reduction problems, providing a possible alternative to existing **public - key** encryption algorithms and **digital signatures** such as RSA and DSS. (22 Refs)
Subfile: B C
Descriptors: computational complexity; data privacy; **public key** cryptography
Identifiers: **public - key** cryptosystems; **lattice** reduction problems; trapdoor one-way function; **public - key** encryption; **digital signatures** ; conjectured computational difficulty; RSA; DSS
Class Codes: B6120B (Codes); C6130S (Data security); C4240C (Computational complexity)

21/5/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

5710015 INSPEC Abstract Number: B9711-0100-034, C9711-6130S-023
Title: Advances in Cryptology - CRYPTO'97. 17th Annual International Cryptology Conference. Proceedings
Editor(s): Kaliski, B.S., Jr.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1997 Country of Publication: Germany xii+537 pp.
ISBN: 3 540 63384 7 Material Identity Number: XX97-02096
Conference Title: Advances in Cryptology - CRYPTO'97. 17th Annual International Cryptology Conference. Proceedings
Conference Date: 17-21 Aug. 1997 Conference Location: Santa Barbara, CA, USA
Language: English Document Type: Conference Proceedings (CP)
Abstract: The following topics were dealt with: complexity theory; cryptographic primitives; **lattice** -based cryptography; **digital signatures** ; cryptanalysis of **public key** cryptosystems; information theory; elliptic curve implementation; number-theoretic systems; distributed cryptography; hash functions; cryptanalysis of secret key cryptosystems.
Subfile: B C
Descriptors: computational complexity; cryptography; information theory; number theory; **public key** cryptography
Identifiers: cryptology; complexity theory; cryptographic primitives; **lattice** -based cryptography; **digital signatures** ; cryptanalysis; **public key** cryptosystems; information theory; elliptic curve implementation; number-theoretic systems; distributed cryptography; hash functions; secret key cryptosystems
Class Codes: B0100 (General electrical engineering topics); B6120B (Codes); B6110 (Information theory); C6130S (Data security); C1260 (Information theory)

21/5/4 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03412000 JICST ACCESSION NUMBER: 97A0959599 FILE SEGMENT: JICST-E
Information and Network Equipment. Fundamentals of the Information Security and its Trends.
KASAHARA MASAO (1)
(1) Kyoto Inst. of Technol.
Nisshin Denki Giho(Nissin Electric Review), 1997, VOL.42,NO.2, PAGE.32-37, REF.13
JOURNAL NUMBER: S0817BAJ ISSN NO: 0549-5377 CODEN: NIDGA
UNIVERSAL DECIMAL CLASSIFICATION: 681.3:654 681.3.02-759
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Commentary
MEDIA TYPE: Printed Publication
ABSTRACT: Nowadays cryptography and information security plays a more and more important role for establishing secure information networks. In this paper we discuss the followings; (1) News topics such as ZKIP(Zero Knowledge Interactive Proof), ID base-crypto system, electronic cash etc. including brief survey on elliptic cipher, quantum cipher, **lattice** cipher etc. (2) Basic technologies of cryptography and information security. (3) Practical aspects of the technology of cryptography and information security such as its application to network security, image encryption etc. (4) Personal review on future information network society. (author abst.)
DESCRIPTORS: computer security; computer network; cryptogram; data protection; **public key** cryptography; security system; image; video

telephone; multi-media; information society; **digital signature** ; protocol; algorithm; theory; authentication; internet; cryptology
BROADER DESCRIPTORS: security; guarantee; communication network; information network; network; protection; system; voice communication; telecommunication; picture communication; information media; society; rule
CLASSIFICATION CODE(S): JC03000K; JD01020V

21/5/5 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2004 INIST/CNRS. All rts. reserv.

13225934 PASCAL No.: 97-0493436
Positive applications of lattices **to cryptography**
MFCS '97 : mathematical foundations of computer science 1997 : Bratislava, August 25-29, 1997
DWORK C
PRIVARA Igor, ed; RUZICKA Peter, ed
IBM Almaden Research Center , Unknown
Mathematical foundations of computer science. International symposium, 22 (Bratislava SVK) 1997-08-25
Journal: Lecture notes in computer science, 1997, 1295 44-51
ISBN: 3-540-63437-1 ISSN: 0302-9743 Availability: INIST-16343; 354000068068640050
No. of Refs.: 26 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany; United States
Language: English
We describe constructions of several cryptographic primitives, including hash functions, **public key** cryptosystems, pseudo-random bit generators, and **digital signatures** , whose security depends on the assumed worst-case or average-case hardness of problems involving **lattices** .
English Descriptors: Computer theory; Computational complexity; Hash coding ; Cryptography

French Descriptors: Informatique theorique; Complexite calcul; Hash coding; Cryptographie

Classification Codes: 001D02A05

21/5/6 (Item 1 from file: 266)
DIALOG(R)File 266:FEDRIP

00172793
IDENTIFYING NO.: 0093029 AGENCY CODE: NSF
CAREER: Geometric Methods in Cryptography
PRINCIPAL INVESTIGATOR: Micciancio, Daniele
PERFORMING ORG.: University of California-San Diego, Computer Science and Engineering, La Jolla, CA 92093-0114
PROJECT MONITOR: Sloan, Robert
SPONSORING ORG.: National Science Foundation, CCR, 4201 Wilson Boulevard , Arlington, Virginia 22230
DATES: 20010215 TO 20030131 FY : 2001 FUNDS: $360,000 (300000)
SUMMARY: As more and more people use computer networks to exchange confidential data and perform business transactions, **public key** cryptography is rapidly becoming one of the most critical tools in today's electronic world. Using cryptography it is possible to perform many important tasks ranging from electronic voting, to **digital** contract **signing** , secure virtual conferences on public networks and many more. All these applications ultimately rely on the security of the underlying cryptographic primitives (i.e. the fundamental building blocks using which all other more complex cryptographic applications are built). This research

involves the study of computational problems from an area of mathematics called geometry of numbers that can be used both to design new cryptographic primitives, and to test old ones and assess their security. The investigators study the complexity of point **lattices** . These are geometric objects that can be described as the set of intersection points of a regular n-dimensional grid. This research involves both the identification of hard **lattice** problems, and the search for better algorithms to solve **lattice** problems that admit efficient solution. Hard **lattice** problems are subsequently used to design new cryptographic functions, while new **lattice** algorithms are used to design new cryptanalytic attacks against existing cryptographic primitives.

21/5/7 **(Item 1 from file: 239)**
DIALOG(R)File 239:Mathsci
(c) 2004 American Mathematical Society. All rts. reserv.

02865929 MR 99a#94041
Advances in cryptology---CRYPTO '97.
Proceedings of the 17th Annual International Cryptology Conference held in Santa Barbara, CA, August 17--21, 1997. Edited by Burton S. Kaliski, Jr.
Contributors: Kaliski, Burton S., Jr.
Publ: Springer-Verlag, Berlin,
1997, xii+540 pp. ISBN: 3-540-63384-7
Series: Lecture Notes in Computer Science, 1294.
Price: $79.00.
Language: English
Document Type: Book; Proceedings
Journal Announcement: 9815
Advances in cryptology---CRYPTO '97; Conference: Cryptology,; Santa Barbara, CA,; Lecture Notes in Computer Science, 17th Annual International, CRYPTO '97 1997 1294
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (68 lines)
The 16th Conference has been reviewed [MR 98f:94001].\}
Contents: Mikael Goldmann and Mats Naslund, The complexity of computing hard core predicates (1--15); Eiichiro Fujisaki and Tatsuaki Okamoto, Statistical zero knowledge protocols to prove modular polynomial relations (16--30); Giovanni Di Crescenzo, Tatsuaki Okamoto and Moti Yung, Keeping the SZK-verifier honest unconditionally (31--45); Oded Goldreich, On the foundations of modern cryptography (46--74); Donald Beaver, Plug and play encryption (75--89); Ran Canetti, Cynthia Dwork, Moni Naor and Rafail Ostrovsky, Deniable encryption (90--104); Oded Goldreich, Shafi Goldwasser and Shai Halevi, Eliminating decryption errors in the Ajtai-Dwork cryptosystem (105--111); Oded Goldreich, Shafi Goldwasser and Shai Halevi, **Public - key** cryptosystems from **lattice** reduction problems (112--131); Rosario Gennaro, Hugo Krawczyk and Tal Rabin, RSA-based undeniable signatures (132--149); Ari Juels, Michael Luby and Rafail Ostrovsky, Security of blind **digital signatures** (extended abstract) (150--164).
Yuliang Zheng, Digital signcryption or how to achieve cost(signature \& encryption) $\ll$ cost(signature) + cost(encryption) (165--179); Rosario Gennaro and Pankaj Rohatgi, How to **sign digital** streams (180--197); Phong Nguyen and Jacques Stern, Merkle-Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations (198--212); Thomas A. Berson, Failure of the McEliece **public - key** cryptosystem under message-resend and related-message attack (213--220); Jean-Francois Misarsky, A multiplicative attack using LLL algorithm on RSA signatures with redundancy (221--234); D. Bleichenbacher, On the security of the KMOV **public key** cryptosystem (235--248); Chae Hoon Lim and Pil Joong Lee, A key recovery attack on discrete log-based schemes using a prime order subgroup (249--263); Adam Young and Moti Yung, The prevalence of kleptographic attacks on discrete-log based cryptosystems (264--276); Mihir Bellare, Shafi Goldwasser and Daniele Micciancio, ``Pseudo-random'' number generation within cryptographic algorithms: the DDS case (277--291); Christian Cachin and Ueli Maurer, Unconditional security against memory-bounded adversaries (292--306).
Ueli Maurer and Stefan Wolf, Privacy amplification secure against active adversaries (307--321); Moni Naor and Benny Pinkas, Visual authentication

and identification (322--336); Gilles Brassard, Quantum information processing: the good, the bad and the ugly (337--341); Jorge Guajardo and Christof Paar, Efficient algorithms for elliptic curve cryptosystems (342--356); Jerome A. Solinas, An improved algorithm for arithmetic on a family of elliptic curves (357--371); Tsuyoshi Takagi, Fast RSA-type cryptosystems using n-adic expansion (372--384); Johannes Buchmann and [illegible] Paulus, A one way function based on ideal arithmetic in number [illegible] (385--394); Shlomi Dolev and Rafail Ostrovsky, Efficient anonymous [illegible] and reception (extended abstract) (395--409); Jan Camenisch and [illegible], Efficient group signature schemes for large groups (extended abstract) (410--424); Dan Boneh and Matthew Franklin, Efficient generation of shared RSA keys (extended abstract) (425--439).

Yair Frankel, Peter Gemmell, Philip D. MacKenzie and Moti Yung, Proactive RSA (440--454); Ran Canetti, Towards realizing random oracles: hash functions that hide all partial information (455--469); Mihir Bellare and Phillip Rogaway, Collision-resistant hashing: towards making UOWHFs practical (470--484); Lars Knudsen and Bart Preneel, Fast and secure hashing based on codes (485--498); Jovan Dj. Golic and Renato Menicocci, Edit distance correlation attack on the alternating step generator (499--512); Eli Biham and Adi Shamir, Differential fault analysis of secret key cryptosystems (513--525); David Wagner, Bruce Schneier and John Kelsey, Cryptanalysis of the cellular message encryption algorithm (526--537).

40/5/7 **(Item 2 from file: 94)**
DIALOG(R)File 94:JICST-EPlus

03602709 JICST ACCESSION NUMBER: 98A0195913 FILE SEGMENT: JICST-E
Development of new public - key **cryptosystems.**
KOBAYASHI KUNIKATSU (1)
(1) Yamagata Univ., Fac. of Eng.
Denki Tsushin Fukyu Zaidan Kenkyu Chosa Hokokusho, 1998, NO.12, PAGE.575-587, FIG.16, TBL.4
JOURNAL NUMBER: J0374AAF ISSN NO: 0918-7332
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: A key selection encoding method which carried out encoding by opening multiple cipher keys to public and by selecting any one of key among them, was proposed. When there is the alternative of the cipher key, ambiguity can be generated, which makes the decoding of the cipher difficult. In a NAPZAP cipher including the vector which is not a super-increase to be used as noise, decoding rate in LLL (**lattice basis** reduction) algorithm lowers, and higher safety than before can be obtained.
DESCRIPTORS: **public key** cryptography; safety; decoding; algorithm; theory; cryptogram; cryptography key; cryptology
BROADER DESCRIPTORS: property; modification; signal processing; treatment
CLASSIFICATION CODE(S): ND02030R

40/5/20 (Item 4 from file: 239)
DIALOG(R)File 239:Mathsci

03021784 MR 2000e#94041

Selected areas in cryptography.

Papers from the 5th Annual International Workshop (SAC '98) held at Queen's University, Kingston, ON, August 17--18, 1998. Edited by Stafford Tavares and Henk Meijer.

Contributors: Tavares, Stafford; Meijer, Henk
Publ: Springer-Verlag, Berlin,
1999, x+377 pp. ISBN: 3-540-65894-7
Series: Lecture Notes in Computer Science, 1556.
Price: $62.00.
Language: English
Document Type: Book; Proceedings
Journal Announcement: 200002
Selected areas in cryptography; Workshop: Selected Areas in Cryptography,; Lecture Notes in Computer Science,; Kingston, ON, 5th Annual International, SAC '98 1556 1998
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (49 lines)

```
File 347:JAPIO Oct 1976-2003/Oct(Updated 040202)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200412
         (c) 2004  Thomson Derwent

Set      Items   Description
S1       45511   LATTICE? ? OR LATICE? ?
S2      287037   BASES OR BASIS
S3        2296   S2(5N)(LONG??? OR LARGE??)
S4        2052   S2(5N)(SMALL??? OR SHORT???)
S5        3452   (DIGITAL? OR ELECTRONIC?)(3N)(SIGN OR SIGNS OR SIGNED OR S-
             IGNING OR SIGNER OR SIGNATURE? ?)
S6        2872   PUBLIC()KEY? ? OR (ASYMMETRIC? OR TWO(W)KEY? ?)(3N)(CRYPT?
             OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
              ENCOD? OR SCRAMBL?)
S7        6677   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
              ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
             OR UNSCRAMBL?
S8         611   S1 AND S2
S9           3   S1 AND S3
S10          7   S1 AND S4
S11          1   S9 AND S10
S12          1   S1 AND S5
S13       1991   (TWO OR DUAL? OR TWIN OR MULTIPL? OR PLURAL? OR DIFFERENT)-
             (5W)S1
S14         36   S2 AND S13
S15          1   S6:S7 AND S14
S16          3   S1 AND S6
S17         17   S1 AND S7
S18         26   S9:S12 OR S15:S17
```

18/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

07748442 **Image available**
METHOD AND APPARATUS FOR EMBEDDING **ENCRYPTED** IMAGE OF SIGNATURE AND OTHER DATA ON CHECK

PUB. NO.: 2003-242347 [JP 2003242347 A]
PUBLISHED: August 29, 2003 (20030829)
INVENTOR(s): COUSINS STEVE B
BREIDENBACH JEFF
JAGANNATHAN RANGASWAMY
APPLICANT(s): XEROX CORP
APPL. NO.: 2002-363007 [JP 2002363007]
FILED: December 13, 2002 (20021213)
PRIORITY: 01 014486 [US 200114486], US (United States of America), December 14, 2001 (20011214)
INTL CLASS: G06F-017/60; G06T-001/00; G09C-001/00; G09C-005/00; H04L-009/32; H04N-001/387

ABSTRACT
PROBLEM TO BE SOLVED: To prevent alteration about a negotiable instrument or the like.
SOLUTION: Glyph marks 21 are formed as a fine pattern on a substrate 24. The glyph marks 21 are comprised of slash-like glyphs 22 arranged in a **lattice** shape, and in the glyphs 22, there are forward slashes representing '1' and backward slashes representing '0'. Binary values are represented by combining both forward and backward slashes. Decoding the glyph marks 21 creates a glyph code pattern 25. By using the glyph code pattern, a payor's signature is digitized, **encrypted** , made to be a glyph and embedded on the front surface of a check. When the check is presented to a bank for payment, a teller using a decoding device, decodes the digitized signature, and sees a human-readable image of the digitized signature on a screen for comparison with the payor's handwritten signature.

18/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

06815274 **Image available**
METHOD AND DEVICE FOR EVALUATING SECRECY SAFETY OF SECRET KEY IN **PUBLIC KEY CIPHERING** SYSTEM

PUB. NO.: 2001-042767 [JP 2001042767 A]
PUBLISHED: February 16, 2001 (20010216)
INVENTOR(s): NAGASE HIROSHI
APPLICANT(s): KANAZAWA INST OF TECHNOLOGY
APPL. NO.: 11-246047 [JP 99246047]
FILED: July 27, 1999 (19990727)
INTL CLASS: G09C-001/00; H04L-009/08

ABSTRACT
PROBLEM TO BE SOLVED: To evaluate secrecy safty of a **public key** and a secret key used in a **public key ciphering** system based on the difficulty of factorization in prime factors like an RSA **ciphering** system by high-speed arithmetic processing.

SOLUTION: According to this evaluation method, the secrecy safty of a secret key is evaluated by judging a composite number z, regarding the composite number z consisting of a product of large prime factors x, y forming a secret key and composing a **public key** , as factor candidate **lattice** points Pmn adopting the prime factor values as plane coordinates, performing remainder arithmetic calculation for the composite number z with

an arbitrary prime number pn as the modulus and selecting a factor candidate evaluation selecting **lattice** point Q35 from many factor candidate **lattice** points Pmn, setting a hyperbola presenting z=x.y and a searching straight line passing through the factor candidate evaluation selecting **lattice** point Q35, setting the grandient of the searching straight line brought to close the straight line gradient of a local line segment of the hypabola in the neighborhood of the factor candidate evaluation selecting **lattice** point Q35 to be searched, expanding the searched range by searching it while sequentially calculating whether or not the intersection point of the above hypabola and the searching straight line matches with the factor candidate evaluation selecting **lattice** point Q35, and being based on the expansion result of the searched range.

18/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO

02411166 **Image available**
HIGH SPEED LOGICAL ELEMENT

PUB. NO.: 63-028066 [JP 63028066 A]
PUBLISHED: February 05, 1988 (19880205)
INVENTOR(s): FURUYA KAZUHITO
APPLICANT(s): TOKYO INST OF TECHNOL [352383] (A Japanese Government or Municipal Agency), JP (Japan)
APPL. NO.: 61-170748 [JP 86170748]
FILED: July 22, 1986 (19860722)
INTL CLASS: [4] H01L-029/72; H01L-029/205
JAPIO CLASS: 42.2 (ELECTRONICS -- Solid State Components)
JOURNAL: Section: E, Section No. 629, Vol. 12, No. 234, Pg. 149, July 05, 1988 (19880705)

ABSTRACT

PURPOSE: To enable a logical element to become a high speed one, by controlling output current by changing wavelength of electron waves while constant current is made to flow inside the element.

CONSTITUTION: A barrier layer is formed of semiconductor having **larger** gap energy than **bases** 1 and 2. For example, this can be realized by using Al(sub x) Ca(sub 1-x) As to perform **lattice** matching and to obtain hetero structure having different gap energy. The gap layer is made to be 500-1000 angstroms or so thick. Periodical structure is formed of layers whose gap energy changes in **lattice** shapes formed between the barrier and the base 2. The gap energy difference needs to be approximately switching voltage (0.05V) or more, and the thickness of the layer needs to be the one (50-100 angstroms) in which tunnel current becomes fully small. when foward bias is applied between an emitter and a base 1, electrons are injected into the base 1, and then constant current depending on diffusion flows toward the other-sided base 2. At that time, voltage is applied between the bases 1 and 2 to control electron speed, that is, wavelength.

18/5/5 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015942040
WPI Acc No: 2004-099881/200411
XRPX Acc No: N04-079486
Lattice **particle** cipher **counterfeit-proofing method**
Patent Assignee: LIAO Y (LIAO-I)
Inventor: LIAO Y
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week

CN 1455366 A 20031112 CN 2002116052 A 20020503 200411 B

Priority Applications (No Type Date): CN 2002116052 A 20020503
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
CN 1455366 A G06K-009/00

Abstract (Basic): CN 1455366 A
NOVELTY - The invention relates to the method for anti false product by using the anti false labeling printed according to the anti false information composed of the characters of fine particles contained in the paper made from specific material and the individualized digital **cipher** code of the product. The information said above is input, stored and processed in measured description by the computer. The consumer can check the quantity of the fine particles in the grid of the label directly, or through telephone, networked computer, fax validate the information of the **cipher** code from the database so asto reach the goal of validating whether the product is true or false.
DwgNo 0/0
Title Terms: **LATTICE** ; PARTICLE; **CIPHER** ; COUNTERFEIT; PROOF; METHOD
Derwent Class: P85; T04
International Patent Class (Main): G06K-009/00
International Patent Class (Additional): G06F-017/30; G09F-003/00
File Segment: EPI; EngPI

18/5/6 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015431729 **Image available**
WPI Acc No: 2003-493871/200346
XRPX Acc No: N03-392344
Signing **and verifying** digital **document using NTRU or convolution modular lattic vector crypotgraphic system whereby a signatory's private key provides a** short **generating** basis **for an NTRU** lattice
Patent Assignee: NTRU CRYPTOSYSTEMS INC (NTRU-N)
Inventor: HOFFSTEIN J; HOWGRAVE-GRAHAM N A; PIPHER J C; SILVERMAN J H; WHYTE W J
Number of Countries: 096 Number of Patents: 002
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
WO 200350998 A1 20030619 WO 2002US38640 A 20021206 200346 B
US 20030120929 A1 20030626 US 2001338330 P 20011207 200355
US 2002313082 A 20021206

Priority Applications (No Type Date): US 2001338330 P 20011207; US 2002313082 A 20021206
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
WO 200350998 A1 E 54 H04L-009/30
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SI SK SL SZ TR TZ UG ZM ZW
US 20030120929 A1 H04L-009/00 Provisional application US 2001338330

Abstract (Basic): WO 200350998 A1
NOVELTY - Involves using the signatory's private key as a **short** generating **basis** for an NTRU (convolution modular) **lattice** and thier **public key** as a much longer generating bais for the same **lattice** . The **signature** on a **digital** document is a vector in the **lattice** with three properties: it is attached to the **digital** document is **signed** , it demonstrates an ability to solve a general

closest vector problem in the **lattice** , and that a private vector of a general NTRU **lattice** can be used first to construct a complete **short basis** for the **lattice** .

USE - To **sign** and verify a **digital** document.

ADVANTAGE - Provides straightforward linkage between the signature and the closest vector problem in the underlying NTRU **lattice** .

DESCRIPTION OF DRAWING(S) - The drawing shows a flow diagram of the method.

pp; 54 DwgNo 2/4

Title Terms: SIGN; VERIFICATION; DIGITAL; DOCUMENT; CONVOLUTE; MODULE; VECTOR; SYSTEM; PRIVATE; KEY; SHORT; GENERATE; BASIS; **LATTICE**

Derwent Class: W01

International Patent Class (Main): H04L-009/00; H04L-009/30

International Patent Class (Additional): H04L-009/32

File Segment: EPI

18/5/7 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015199123 **Image available**

WPI Acc No: 2003-259657/200326

Related WPI Acc No: 2002-343136; 2003-259656

XRPX Acc No: N03-205847

Quantum dot photon source for e.g. optical quantum cryptography **has quantum dot excited by pulsed radiation source related to the recombination and relaxation times of the dot**

Patent Assignee: TOSHIBA RES EURO LTD (TOKE)

Inventor: HOGG R A; SHIELDS A J

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2377551	A	20030115	GB 9927690	A	19991123	200326	B
			GB 200224125	A	20021016		
GB 2377551	B	20031112	GB 9927690	A	19991123	200375	
			GB 200224125	A	20021016		

Priority Applications (No Type Date): GB 9927690 A 19991123; GB 200224125 A 20021016

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2377551	A		61	H01L-033/00	Div ex application GB 9927690
GB 2377551	B			H01L-033/00	Div ex application GB 9927690

Abstract (Basic): GB 2377551 A

NOVELTY - The quantum dot photon source comprises: (a) a quantum dot; and (b) means for supplying carriers, comprising incident radiation pulsed at specific times to exciting a predetermined number of carriers into first and second energy levels to allow recombination of carriers in quantum dot to emit at least one photon. The quantum dot is encapsulated between two layers having a different **lattice** constant to the quantum dot.

DETAILED DESCRIPTION - The pulse of the excitation radiation has a duration which is less than the relaxation time of a carrier which it excites in the quantum dot. The time between leading edges of successive pulses is greater than the recombination time of an electron and a hole in a quantum dot. The incident radiation has a predefined polarization. The pulsed radiation can be a continuous wave laser diode that whereby the quantum dot filter is modulated through an AC energy source or the radiation source can be a pulsed laser diode.

USE - The single photon source can be used for optical quantum **cryptography** or for optical imaging, spectroscopy, laser ranging and metrology.

ADVANTAGE - The single photon source is configured to allow emission of a predetermined number of photons at predetermined times. These sources have a reduced shot noise.

DESCRIPTION OF DRAWING(S) - The drawing shows a single photon

emitter in accordance with an embodiment of the present invention located within a resonant cavity.
pp; 61 DwgNo 4/22
Title Terms: QUANTUM; DOT; PHOTON; SOURCE; OPTICAL; QUANTUM; QUANTUM; DOT; EXCITATION; PULSE; RADIATE; SOURCE; RELATED; RECOMBINATION; RELAX; TIME; DOT
Derwent Class: S02; S03; U12; V08; W01; W02
International Patent Class (Main): H01L-033/00
File Segment: EPI

18/5/12 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013765404 **Image available**
WPI Acc No: 2001-249615/200126
XRPX Acc No: N01-177942
Security assessment procedure secret key in communication network, involves detecting search lines with gradient near hyperbola area, to set search range and accordingly lattice **points are estimated**
Patent Assignee: UNIV KANAZAWA KOGYO (UYKA-N)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001042767	A	20010216	JP 99246047	A	19990727	200126	B

Priority Applications (No Type Date): JP 99246047 A 19990727
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001042767	A		11	G09C-001/00	

Abstract (Basic): JP 2001042767 A
NOVELTY - The search lines (L10) extending along the selected factor classification **lattice** points (Q35,Q52) distributed on the evaluation graph is identified. The search line with gradient near the hyperbola area is detected and accordingly enlarged search range is set. The **lattice** points along the detected line are estimated relevant to search range, to evaluate key security.
DETAILED DESCRIPTION - The evaluation factor classification **lattice** points (Pmn) are computed by synthesizing the maximum prime numbers (x,y) of key. The value of each **lattice** point is estimated, based on the coordinates of each point. The planar coordinates of the **lattice** points is estimated using positional information of each point and relation Z is equal to xy where z is synthetic number value. Hyperbola is drawn along the points based on the relation, to obtain several lines. An INDEPENDENT CLAIM is also included for security assessment apparatus of secret key.
USE - For evaluating security of secret keys used in **encryption** management of communication network used for electronic commercial transactions.
ADVANTAGE - The key security is judged correctly and quantitatively, by enlarged search algorithm.
DESCRIPTION OF DRAWING(S) - The figure shows the graph representing the search line evaluation procedure. (The drawing includes non-English language text).
Search lines (L10)
Lattice points (Q35,Q52)
pp; 11 DwgNo 3/13
Title Terms: SECURE; ASSESS; PROCEDURE; SECRET; KEY; COMMUNICATE; NETWORK; DETECT; SEARCH; LINE; GRADIENT; HYPERBOLIC; AREA; SET; SEARCH; RANGE; ACCORD; **LATTICE** ; POINT; ESTIMATE
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00
International Patent Class (Additional): H04L-009/08
File Segment: EPI; EngPI

18/5/13 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012965852
WPI Acc No: 2000-137701/200013
XRPX Acc No: N00-102964
Periodically deciphered **anti-faking printings and preparation thereof**
Patent Assignee: BAOZHEN SCI & TECHNOLOGY DEV CO LTD GUAN (BAOZ-N)
Inventor: CHEN J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CN 1235096	A	19991117	CN 99104584	A	19990423	200013	B

Priority Applications (No Type Date): CN 99104584 A 19990423
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CN 1235096	A		1	B41M-003/00	

Abstract (Basic): CN 1235096 A
NOVELTY - An antiforge printed article **deciphered** in instalments on the **basis** of reproducing the colour and layers of normal printed articles and playing the antiforge role of netted antiforge printed articles. **Different cipher** units are distributed in **lattices** at different regions on pages, with its print plate made up by the computer.
USE - An antiforge printed article for resisting against counterfeits.
ADVANTAGES - High antiforge power, easy recognition, and very high potential power for resisting against counterfeits.
Dwg.0
Title Terms: PERIOD; ANTI; PRINT; PREPARATION
Derwent Class: P75; T01
International Patent Class (Main): B41M-003/00
File Segment: EPI; EngPI

18/5/14 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011822658 **Image available**
WPI Acc No: 1998-239568/199821
XRPX Acc No: N98-189513
Cryptographic **communication system - has** cryptographic **communication system with mechanism for generating** public key **and private key, based on worst case, with mechanism for executing** cryptographic **communication protocol using keys**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: AJTAI M
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5737425	A	19980407	US 96646806	A	19960521	199821	B

Priority Applications (No Type Date): US 96646806 A 19960521
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5737425	A		19	H04K-001/00	

Abstract (Basic): US 5737425 A
The **cryptographic** communication system comprises a communication channel. There is a mechanism for generating a **public key** and a corresponding private key, based on an instance of a problem. The problem is difficult to solve in the worst case. The instance of the problem being difficult to solve is commensurate with the difficulty of the worst case solution of the problem.

There is a mechanism for carrying out a **cryptographic** communication protocol using the public and private keys generated, with another **cryptographic** communication system, over the communication channel. The mechanism for generating, which includes the **public key** generator, preferably includes a **lattice** .

USE - For **cryptography** and **cryptosystems** .

ADVANTAGE - Provides system with security based on difficulty of worst case problem.

Dwg.1/7

Title Terms: **CRYPTOGRAPHIC** ; COMMUNICATE; SYSTEM; **CRYPTOGRAPHIC** ; COMMUNICATE; SYSTEM; MECHANISM; GENERATE; PUBLIC; KEY; PRIVATE; KEY; BASED; WORST; CASE; MECHANISM; EXECUTE; **CRYPTOGRAPHIC** ; COMMUNICATE; PROTOCOL; KEY

Derwent Class: W01

International Patent Class (Main): H04K-001/00

File Segment: EPI

18/5/15 **(Item 11 from file: 350)**

011693954

WPI Acc No: 1998-110864/199810

XRAM Acc No: C98-036518

XRPX Acc No: N98-088692

Encryption **and** decryption **system for distributing MIDI files - involves** encrypting **MIDI streams at source and** decrypting **them only within downloaded integral** decrypters **-MIDI-decoders**

Patent Assignee: TOYOTA JIDOSHA KK (TOYT); TOYOTA SCHOOL FOUND (TOYO-N); GH TOYOTA KAKUEN (TOYO-N); SUZUKI T (SUZU-I); VAN DRENT W (VDRE-I)

Inventor: SUZUKI T; VAN DRENT W

Number of Countries: 021 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9802876	A1	19980122	WO 97JP2415	A	19970711	199810	B
EP 911821	A1	19990428	EP 97930769	A	19970711	199921	
			WO 97JP2415	A	19970711		
JP 10505843	X	19990921	WO 97JP2415	A	19970711	199950	
			JP 98505843	A	19970711		
US 6163509	A	20001219	WO 97JP2415	A	19970711	200102	
			US 98220767	A	19981228		
KR 2000023720	A	20000425	KR 99700180	A	19990111	200107	
US 20020027836	A1	20020307	WO 97JP2415	A	19970711	200221	
			US 98220767	A	19981228		
			US 2000819068	A	20001212		

Priority Applications (No Type Date): JP 96182019 A 19960711

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9802876	A1	E	59	G11B-011/10	
Designated States (National): JP KR SG US					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 911821	A1	E		G11B-011/10	Based on patent WO 9802876
Designated States (Regional): DE FR GB NL					
JP 10505843	X			G11B-011/10	Based on patent WO 9802876
US 6163509	A			G11B-011/00	Cont of application WO 97JP2415
KR 2000023720	A			G11B-011/10	
US 20020027836	A1			G11B-011/00	Cont of application WO 97JP2415 Cont of application US 98220767 Cont of patent US 6163509

Abstract (Basic): WO 9802876 A

A Co thin film for magneto-optical recording is made of a material having a large polar rotation angle in an ultraviolet region to achieve high density recording. A Co thin film (14) is vacuum deposited on an Si substrate with a Cu seed layer (12) therebetween. The orientation of

the Si substrate is (100) or (111). The thicknesses of the Cu seed layer (12) and the Co thin film (14) are both approx. 100 nm. The Co thin film (14) is a single crystal thin film having a face-centred cubic **lattice** structure with an orientation of (100) or (111). Such a Co thin film (14) has a polar rotation angle of maximum 0.4 deg. in the ultraviolet wavelength region of 200-230 nm.

Dwg.0/15

Title Terms: **ENCRYPTION** ; **DECRYPTER** ; SYSTEM; DISTRIBUTE; MIDI; FILE; MIDI; STREAM; SOURCE; INTEGRAL; MIDI; DECODE
Derwent Class: L03; P73; T03; V02; W04
International Patent Class (Main): G11B-011/00; G11B-011/10
International Patent Class (Additional): B32B-003/02
File Segment: CPI; EPI; EngPI

18/5/17 **(Item 13 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

008880409 **Image available**
WPI Acc No: 1992-007680/199201
XRPX Acc No: N92-005875

Image coding method and apparatus - generates output images from weighted sums of input image, weights are sets of two-dimensional irreducible coefficients

Patent Assignee: AWARE INC (AWAR-N)
Inventor: PLUMMERLIN D C; POLLEN D; RESNIKOFF H L
Number of Countries: 017 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9119271	A	19911212				199201	B
AU 9180770	A	19911231				199215	
US 5101446	A	19920331	US 90531468	A	19900531	199216	
IL 98249	A	19931228	IL 98249	A	19910523	199403	N

Priority Applications (No Type Date): US 90531468 A 19900531; IL 98249 A 19910523
Cited Patents: 1.Jnl.Ref; US 4802110; US 4805129; US 4817182
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9119271	A				
Designated States (National): AU BR JP KR SU					
Designated States (Regional): AT CH ES FR GB GR IT LU NL SE					
US 5101446	A		28		
IL 98249	A			H04N-001/41	

Abstract (Basic): WO 9119271 A

Projection apparatus (900) for coding two-dimensional array IM includes a device (905) for storing a 2 x 2 matrix S. Modulus of det S greater than 1 and S maps any **lattice** point in a Z-dimensional **lattice** into another point in the **lattice** . A second storage device (906) stores a set of irreducible sealing coefficients (am) having a multiplier M = modulus of det S. A receiving device (907) receives the two-dimensional data array.

A further device (904) generates a low-frequency data array Vm wherein Vm = (EK aK I sm + K)/M and K runs over all values for which aK is not zero. A device outputs the low-frequency data array.

ADVANTAGE - Uses orthonormal transformation of image utilising **basis** functions with support that is **small** compared to size of image. Compression ratio may be selected in increments other than factors of four. (68pp Dwg.No.9/12)

Title Terms: IMAGE; CODE; METHOD; APPARATUS; GENERATE; OUTPUT; IMAGE; WEIGHT; SUM; INPUT; IMAGE; WEIGHT; SET; TWO-DIMENSIONAL; COEFFICIENT
Derwent Class: T01; W02
International Patent Class (Main): H04N-001/41
International Patent Class (Additional): G06K-009/36; H03M-007/30
File Segment: EPI

18/5/21 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

004033166
WPI Acc No: 1984-178708/198429
XRPX Acc No: N84-133438
Speech enciphering method for transmission over conventional channel - has linear prediction analysis circuit which models input speech spectrum in form of digitised coefficients describing all-pole model
Patent Assignee: STAND TEL CABLE PLC (INTT); STC PLC (STTE)
Inventor: SCOTT M A
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2133255	A	19840718	GB 8236631	A	19821223	198429	B
GB 2133255	B	19860403				198614	

Priority Applications (No Type Date): GB 8236631 A 19821223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2133255	A		5		

Abstract (Basic): GB 2133255 A

The appts. has an analog to digital converter (11) for digitising the speech signals. A linear prediction analysis device (12) derives digital coefficients relating to predetermined characteristics of the digitised signals. The digitised signals are applied to a filter which is weighted with the coefficients. The output of the filter is applied to an inverse filter which is weighted with the **scrambled** coefficients.

The output of the inverse filter is applied to a digital to analog converter (16). The **scrambler** and **unscrambler** allow an operator to set the key stream. The filters are identical adaptive **lattice** filters. The **scrambler** and descrambler also effect a simple binary addition without carry of the predetermined binary key stream to the digital coefficients.

USE - For police mobile radio intended to be secured against casual eavesdropping.

```
File 347:JAPIO Oct 1976-2003/Oct(Updated 040202)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200412
         (c) 2004  Thomson Derwent

Set     Items   Description
S1      45511   LATTICE? ? OR LATICE? ?
S2     287037   BASES OR BASIS
S3       2296   S2(5N)(LONG??? OR LARGE??)
S4       2052   S2(5N)(SMALL??? OR SHORT???)
S5       3452   (DIGITAL? OR ELECTRONIC?)(3N)(SIGN OR SIGNS OR SIGNED OR S-
            IGNING OR SIGNER OR SIGNATURE? ?)
S6       2872   PUBLIC()KEY? ? OR (ASYMMETRIC? OR TWO(W)KEY? ?)(3N)(CRYPT?
            OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
             ENCOD? OR SCRAMBL?)
S7      35607   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
             ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
            OR UNSCRAMBL?
S8       1455   (AUXILIARY OR ALTERNATE OR ALTERNATIVE OR ANOTHER OR OTHER
            OR SEPARATE OR SECOND? OR 2ND OR ADDITIONAL)(5W)S1
S9         29   S2 AND S8
S10         0   S3 AND S8
S11         1   S4 AND S8
S12         0   S5 AND S8
S13         0   S6 AND S8
S14         0   S7 AND S8
S15        29   S9 OR S11
```

Surface acoustic wave device - incorporates K coupled pairs of auxiliary direction couplers in auxiliary acoustic waveguides with reflecting lattice in each and includes auxiliary reflecting structure in each principal and auxiliary acoustic waveguide

15/TI/22 (Item 5 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Image coding method and apparatus - generates output images from weighted sums of input image, weights are sets of two-dimensional irreducible coefficients

15/TI/23 (Item 6 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Heteroepitaxial multilayers with reduced lattice mismatch - prepd. by ion implantation to create defects and amorphising-boundary of layers

15/TI/24 (Item 7 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

High quality character generator - outputs projection start command to filling section in response to end signal from projection section

15/TI/25 (Item 8 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Monitoring occurrence of fire - measuring propagation speed of ultrasonic waves through channels between transmitters and receivers

15/TI/26 (Item 9 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

N-dimensional modular multiprocessor lattice architecture - has system of modules interconnected using dual port memories each dedicated solely to interchange of information between two modules

15/TI/27 (Item 10 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Photoelectric displacement detector with optical lattice - has subsidiary optical lattice divided into sections by phase dividing frame and light receivers corresp. to divided lattices

15/TI/28 (Item 11 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Frame structure for skeletons and inner fitting - has closed triangular bracket, whose shank centre lines brace rectangular pyramid side surfaces

15/TI/29 (Item 12 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Heat-resistant polybutadiene-polystyrene-carboxyl latex - contg. phenolic antioxidant and semi-ester of sulphosuccinic acdi with ethoxylated alcohol

15/TI/1 (Item 1 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

PATTERN FORMING METHOD AND ELECTRON BEAM EXPOSURE DEVICE

15/TI/2 (Item 2 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

METHOD AND DEVICE FOR IMAGE EFFECT

15/TI/3 (Item 3 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

MOVING POINT LOCUS MEASURING METHOD, MOVING POINT LOCUS MEASURING DEVICE, IMAGE PROCESSING METHOD, IMAGE PROCESSING DEVICE, COMPUTER-READABLE RECORDING MEDIUM WITH MOVING POINT LOCUS MEASURING PROGRAM RECORDED THEREON, AND MOVING POINT LOCUS MEASURING PROGRAM

15/TI/4 (Item 4 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

METHOD AND DEVICE FOR INTERPOLATING SPACE DATA, AND ANIMATION MAKING METHOD

15/TI/5 (Item 5 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

METHOD AND APPARATUS FOR INSPECTION OF SCANNING OPTICAL UNIT

15/TI/6 (Item 6 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

CEREBRAL EQUIPOTENTIAL DIAGRAM FORMING APPARATUS AND CERBRRAL EQUIPOTNTIAL CONVERTER

15/TI/7 (Item 7 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

DEVICE FOR REARING ANIMAL

15/TI/8 (Item 8 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

PRESUMING METHOD FOR CURRENT SOURCE OF VITAL ORGANISM ACTIVITY

15/TI/9 (Item 9 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

PRESUMING METHOD FOR CURRENT SOURCE OF VITAL ORGANISM ACTIVITY

15/TI/10 (Item 10 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

X-RAY DIAGNOSTIC DEVICE

15/TI/11 (Item 11 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

MAGNETIC HEAD DRIVING DEVICE

15/TI/12 (Item 12 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

SPHERE TEXTURE MAPPING DEVICE

15/TI/13 (Item 13 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

IMPROVED THERMAL STENCIL PAPER

15/TI/14 (Item 14 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

OPTICAL AUTOMATIC POSITIONING APPARATUS

15/TI/15 (Item 15 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

OPTICAL DISPLACEMENT DETECTOR

15/TI/16 (Item 16 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

METHOD AND APPARATUS FOR SETTING GAP BETWEEN FIRST AND SECOND OBJECTS TO PREDETERMINED VALUE

15/TI/17 (Item 17 from file: 347)
DIALOG(R)File 347:(c) 2004 JPO & JAPIO. All rts. reserv.

OPTICAL DISPLACEMENT DETECTOR

15/TI/18 (Item 1 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Aluminum material as matrix material for forming composites of e.g., mechanical devices e.g., compressor section of gas turbine engine, includes solid solution matrix containing specified amount of aluminum alloy

15/TI/19 (Item 2 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Integrated tablet input appts. with liquid crystal display - includes position detecting function and display function with liquid-crystal display in matrix form with insulating substrate, scanning lines running parallel to substrate

15/TI/20 (Item 3 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

Semiconductor device - has two semiconductor bases **bonded together with their crystal structure differing from each other in section that is perpendicular to bonding surface**

15/TI/21 (Item 4 from file: 350)
DIALOG(R)File 350:(c) 2004 Thomson Derwent. All rts. reserv.

42/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

06145144 E.I. No: EIP02397107087
Title: Combining problem structure with basis reduction to solve a class of hard integer programs
Author: Louveaux, Quentin; Wolsey, Laurence A.
Corporate Source: INMA CORE Universite catholique de Louvain, Louvain-la-Neuve, B-1348, Belgium
Source: Mathematics of Operations Research v 27 n 3 August 2002. p 470-484
Publication Year: 2002
CODEN: MOREDQ ISSN: 0364-765X
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0209W5
Abstract: Recently Aardal et al. (2000) have successfully solved some small, difficult, equality-constrained integer programs by using basis reduction to reformulate the problems as inequality-constrained integer programs in a different space. Here, we adapt their method to solve integer programs that are larger but have special structure. The practical problem motivating this work is a variant of the market share problem. More formally, the problem can be viewed as finding a matrix X is a member of the set of Double-struck Z //+**m**n satisfying XA = C, BX = D, where A, B, C, D are matrices of compatible dimensions, and the approach requires us to find a reduced basis of the lattice script L = left brace X is a member of the set of Double-struck Z **m** multiplied by **n: XA = 0, BX = 0 right brace . The main topic of this paper is a study of the lattice script L . It is shown that an integer basis of script L can be obtained by taking the Kronecker product of vectors from integer **bases** of **two** much **smaller lattices** . Furthermore, the resulting **basis** is a reduced basis if the integer **bases** of the **two small lattices** are reduced **bases** and a suitable ordering is chosen. Finally, some limited computational results are presented showing the benefits of making use of the problem structure. 12 Refs.
Descriptors: *Integer programming; Problem solving; Vectors; Computation theory; Matrix algebra; Set theory; Theorem proving; Algorithms
Identifiers: Polynomial algorithms
Classification Codes:
921.5 (Optimization Techniques); 921.1 (Algebra); 721.1 (Computer Theory (Includes Formal Logic, Automata Theory, Switching Theory & Programming Theory)); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)
921 (Applied Mathematics); 721 (Computer Circuits & Logic Elements)
92 (ENGINEERING MATHEMATICS); 72 (COMPUTERS & DATA PROCESSING)

42/5/7 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2004 INIST/CNRS. All rts. reserv.

14725060 PASCAL No.: 00-0401244
The complexity of some lattice problems
ANTS-IV : algorithmic number theory : Leiden, 2-7 July 2000
BOSMA Wieb, ed
Department of Computer Science and Engineering, State University of New York, Buffalo, NY 14260, United States
Algorithmic number theory. International symposium, 4 (Leiden NLD) 2000-07-02
Journal: Lecture notes in computer science, 2000, 1838 1-32
ISBN: 3-540-67695-3 ISSN: 0302-9743 Availability: INIST-16343; 354000087639230010
No. of Refs.: 66 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English

We survey some recent developments in the study of the complexity of certain lattice problems. We focus on the recent progress on complexity results of intractability. We will discuss Ajtai's worst-case/average-case connections for the shortest vector problem, similar results for the closest vector problem and **short basis** problem, NP-hardness and non-NP-hardness, transference theorems between primal and **dual lattices** , and application to secure cryptography.

45/5/2 (Item 1 from file: 65)
DIALOG(R)File 65:Inside Conferences

03867151 INSIDE CONFERENCE ITEM ID: CN040653880
The Two **Faces of** Lattices **in** Cryptology
Nguyen, P. Q.; Stern, J.
CONFERENCE: Cryptography and lattices-International conference; 1st
LECTURE NOTES IN COMPUTER SCIENCE, 2001; VOL 2146 P: 146-180
New York, Springer, 2001
ISSN: 0302-9743 ISBN: 3540424881
LANGUAGE: English DOCUMENT TYPE: Conference Revised papers
CONFERENCE EDITOR(S): Silverman, J. H.
CONFERENCE SPONSOR: Brown University
CONFERENCE LOCATION: Providence, RI 2001; Mar (200103) (200103)

BRITISH LIBRARY ITEM LOCATION: 5180.185000
NOTE:
Also known as CaLC 2001
DESCRIPTORS: **cryptography** ; CaLC

45/5/3 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7868991 INSPEC Abstract Number: B2004-03-6120D-086, C2004-03-6130S-183
Title: Cryptocomputing **with rationals**
Author(s): Fouque, P.-A.; Stern, J.; Wackers, G.-J.
Author Affiliation: DCSSI Crypto Lab., Paris, France
Conference Title: Financial Cryptography. 6th International Conference, FC 2002. Revised Papers (Lecture Notes in Computer Science Vol.2357) p. 136-46
Editor(s): Blaze, M.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 2003 Country of Publication: Germany viii+299 pp.
ISBN: 3 540 00646 X Material Identity Number: XX-2003-00822
Conference Title: Financial Cryptography. 6th International Conference, FC 2002. Revised Papers
Conference Date: 11-14 March 2002 Conference Location: Southampton, Bermuda
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: In this paper we describe a method to compute with **encrypted** rational numbers. It is well-known that homomorphic schemes allow calculations with hidden integers, i.e. given integers x and y **encrypted** in xi (x0 and xi (y), one can compute the **encrypted** sum xi (x+y) or the **encrypted** product xi (kx) of the **encrypted** integer x and a known integer k without having to **decrypt** the terms xi (x) or xi (y). Such **cryptosystems** have a lot of applications in electronic voting schemes, lottery or in multiparty computation since they allow to keep the privacy of the terms and return the result in **encrypted** form. However, from a practical point of view, it might be interesting to compute with rationals. For instance, a lot of financial applications require algorithms to compute with rational values instead of integers such as bank accounts, electronic purses in order to make payments or micropayments, or secure spreadsheets. We present here a way to solve this problem using the Paillier **cryptosystem** which offers the largest bandwidth among all homomorphic schemes. The method uses **two** -dimensional **lattices** to recover the numerator and denominator of the rationals. Finally we implement this technique and our results in order to build an **encrypted** spreadsheet showing the practical possibilities of the homomorphic properties applied on rationals. (23 Refs)
Subfile: B C
Descriptors: **cryptography** ; Gaussian processes; rational functions
Identifiers: **cryptocomputing** ; rationals; **encrypted** rational numbers; homomorphic schemes; **encrypted** sum; **encrypted** product; **encrypted** integer; **cryptosystems** ; electronic voting scheme; lottery; multiparty

computation; financial applications; bank accounts; electronic purses; secure spreadsheets; Paillier **cryptosystem** ; **two** -dimensional **lattices** ; **encrypted** spreadsheet
Class Codes: B6120D (Cryptography); C6130S (Data security); C4130 (Interpolation and function approximation (numerical analysis))

45/5/4 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

7130209 INSPEC Abstract Number: B2002-02-6210L-001, C2002-02-5620-001
Title: An encryption approach to digital communication by using spatiotemporal chaos synchronization
Author(s): Kuang Jing-Yu; Deng Kun; Huang Rong-Hai
Author Affiliation: Dept. of Electron., Beijing Normal Univ., China
Journal: Acta Physica Sinica vol.50, no.10 p.1856-61
Publisher: Chinese Phys. Soc,
Publication Date: 2001 Country of Publication: China
CODEN: WLHPAR ISSN: 1000-3290
SICI: 1000-3290(2001)50:10L.1856:EADC;1-7
Material Identity Number: A279-2001-021
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: An **encryption** approach to digital communication by using spatiotemporal chaos synchronization is proposed. **Two** one-way coupled map **lattice** (OCOML) systems driven by a chaotic signal are synchronized. The chaotic outputs of the OCOML systems serve as the **encryption** and **decryption** keys and the main secret key is a set of coupling parameters of the OCOML. The advantages of the **cryptosystem** are its high communication efficiency, higher level of security and easy implementation by software. An example of duplex real-time voice communication between two computer users is described. (18 Refs)
Subfile: B C
Descriptors: chaos; computer networks; **cryptography** ; digital communication; synchronisation; telecommunication security; voice communication
Identifiers: **encryption** approach; digital communication; spatiotemporal chaos synchronization; one-way coupled map lattice systems; chaotic signal; chaotic outputs; OCOML systems; **decryption** keys; coupling parameters; communication efficiency; security; duplex real-time voice communication; computer users
Class Codes: B6210L (Computer communications); B6120D (Cryptography); C5620 (Computer networks and techniques)

45/5/5 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6307951 INSPEC Abstract Number: C1999-09-4240C-024
Title: Some recent progress on the complexity of lattice problems
Author(s): Jin-Yi Cai
Author Affiliation: Dept. of Comput. Sci. & Eng., State Univ. of New York, Buffalo, NY, USA
Conference Title: Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat.No.99CB36317) p.158-78
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1999 Country of Publication: USA x+241 pp.
ISBN: 0 7695 0075 7 Material Identity Number: XX-1999-01869
U.S. Copyright Clearance Center Code: 0 7695 0075 7/99/$10.00
Conference Title: Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity. (Formerly: Structure in Complexity Theory Conference)
Conference Sponsor: IEEE Comput. Soc. Tech. Committee on Math. Found.

Comput.; ACM SIGACT; EATCS
Conference Date: 4-6 May 1999 Conference Location: Atlanta, GA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We survey some recent developments in the study of the complexity of lattice problems. After a discussion of some problems on lattices which can be algorithmically solved efficiently, our main focus is the recent progress on complexity results of intractability. We discuss Ajtai's worst-case/average-case connections, NP-hardness and non-NP-hardness, transference theorems between primal and **dual lattices**, and the Ajtai-Dwork **cryptosystem**. (62 Refs)
Subfile: C
Descriptors: computational complexity; **cryptography**
Identifiers: complexity; lattice problems; intractability; NP-hardness; non-NP-hardness; transference theorems; **cryptosystem**
Class Codes: C4240C (Computational complexity); C1260C (Cryptography theory); C6130S (Data security)

45/5/6 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

5862657 INSPEC Abstract Number: B9804-6120B-280, C9804-6130S-053
Title: Finding small roots of univariate modular equations revisited
Author(s): Howgrave-Graham, N.
Author Affiliation: Bath Univ., UK
Conference Title: Cryptography and Coding. 6th IMA International Conference. Proceedings p.131-42
Editor(s): Darnell, M.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1997 Country of Publication: Germany 334 pp.
ISBN: 3 540 63927 6 Material Identity Number: XX97-01681
Conference Title: Proceedings of Cryptography
Conference Date: 17-19 Dec. 1997 Conference Location: Cirencester, UK
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: An alternative technique for finding small roots of univariate modular equations is described. This approach is then compared with that taken in Coppersmith (1996), which links the concept of the **dual lattice** (Cassels, 1971) to the LLL algorithm (Lenstra et al., 1982). Timing results comparing both algorithms are given, and practical considerations are discussed. This work has direct applications to several low-exponent attacks on the RSA **cryptographic** scheme.

48/5/4 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6512531 INSPEC Abstract Number: B2000-04-6120D-018, C2000-04-1260C-012
Title: Generating hard instances of the short basis problem
Author(s): Ajtai, M.
Author Affiliation: IBM Almaden Res. Center, San Jose, CA, USA
Conference Title: Automata, Languages and Programming. 26th International Colloquium, ICALP'99. Proceedings (Lecture Notes in Computer Science Vol.1644) p.1-9
Editor(s): Wiedermann, J.; van Emde Boas, P.; Nielsen, M.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1999 Country of Publication: Germany xiv+718 pp.
ISBN: 3 540 66224 3 Material Identity Number: XX-1999-02197
Conference Title: Proceedings of ICALP'99: 26th International Colloquium on Automata, Languages, and Programming
Conference Date: 11-15 July 1999 Conference Location: Prague, Czech Republic
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: A class of random **lattices** is given in [1] so that: (a) a random **lattice** can be generated in polynomial time together with a short vector in it; and (b) assuming that certain worst-case **lattice** problems have no polynomial time solutions, there is no polynomial time algorithm which finds a short vector in a random **lattice** with a polynomially large probability. We show that **lattices** of the same random class can be generated not only together with a short vector in them, but also together with a **short basis** . The existence of a known **short basis** may make the construction more applicable for **cryptographic** protocols. (7 Refs)
Subfile: B C
Descriptors: computational complexity; **cryptography** ; data structures; probability; protocols
Identifiers: hard instances; **short basis** problem; random **lattices** ; polynomial time; short vector; probability; **cryptographic** protocols
Class Codes: B6120D (Cryptography); B0240Z (Other topics in statistics); B6150M (Protocols); C1260C (Cryptography theory); C4240C (Computational complexity); C1140Z (Other topics in statistics); C5640 (Protocols)

48/5/7 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

10445253 Genuine Article#: 526ZV Number of References: 31
Title: On the design of RSA with short secret exponent
Author(s): Sun HM (REPRINT) ; Yang WC; Laih CS
Corporate Source: Natl Cheng Kung Univ,Dept Comp Sci & Informat Engn,Tainan 701//Taiwan/ (REPRINT); Natl Cheng Kung Univ,Dept Comp Sci & Informat Engn,Tainan 701//Taiwan/; Natl Cheng Kung Univ,Dept Elect Engn,Tainan 701//Taiwan/
Journal: JOURNAL OF INFORMATION SCIENCE AND ENGINEERING, 2002, V18, N1 (JAN), P1-18
ISSN: 1016-2364 Publication date: 20020100
Publisher: INST INFORMATION SCIENCE, ACADEMIA SINICA, TAIPEI 115, TAIWAN
Language: English Document Type: ARTICLE
Geographic Location: Taiwan
Journal Subject Category: COMPUTER SCIENCE, INFORMATION SYSTEMS
Abstract: Based on continued fractions Wiener showed that a typical RSA system can be totally broken if its secret exponent d < N-0.25 where N is the RSA modulus. Recently, based on **lattice** basis reduction, Boneh and Durfee presented a new short secret exponent attack which improves Wiener's bound up to d < N-0.292. In this paper we show that it is possible to use a short secret exponent which is lower than these bounds while not compromising the security of RSA, provided that p and q differ in size and are large enough to defend against factoring algorithms. As an example, an RSA system with d of 192 bits, p of 256

bits, and q of 768 bits is secure against all the existing short secret exponent attacks, On the other hand, in order to balance between and minimize the overall computation of **encryption** and **decryption** , we propose a secure variant of RSA such that both e and d are the same size, log(2)e approximate to log(2)d approximate to 568 for a 1024-bit RSA modulus. Moreover, a generalization of this variant is presented for designing the RSA system with log(2)e + log(2)d approximate to (log(2)N) + l(k) where l(k) is a predetermined constant, e.g., 112. Compared with a typical RSA system in which e is the same order of magnitude as N if d is first selected, these variants of RSA have the advantage that the overall computation can be significantly reduced. As an example, we can construct a secure RSA system with p of 256 bits, q of 768 bits, d of 256 bits, and e of 880 bits.

```
File   8:Ei Compendex(R) 1970-2004/Feb W3
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Jan
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Jan 20
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Feb W4
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Feb W3
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Feb W3
         (c)2004 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2004/Feb W4
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Feb W3
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Feb W3
         (c) 2004 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Jan
         (c) 2004 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 266:FEDRIP 2004/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2004/Feb W2
         (c) 2004 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2004/Jan
         (c) 2004 The HW Wilson Co
File  62:SPIN(R) 1975-2004/Jan W1
         (c) 2004 American Institute of Physics
File 239:Mathsci 1940-2004/Mar
         (c) 2004 American Mathematical Society

Set     Items   Description
S1     944238   LATTICE? ? OR LATICE? ?
S2    1685287   BASES OR BASIS
S3      28437   S2(5N)(LONG??? OR LARGE??)
S4      11718   S2(5N)(SMALL??? OR SHORT???)
S5       9216   (DIGITAL? OR ELECTRONIC?)(3N)(SIGN OR SIGNS OR SIGNED OR S-
            IGNING OR SIGNER OR SIGNATURE? ?)
S6      14874   PUBLIC()KEY? ? OR (ASYMMETRIC? OR TWO(W)KEY? ?)(3N)(CRYPT?
            OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
             ENCOD? OR SCRAMBL?)
S7     166738   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
             ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
            OR UNSCRAMBL?
S8       8716   (AUXILIARY OR ALTERNATE OR ALTERNATIVE OR ANOTHER OR OTHER
            OR SEPARATE OR SECOND? OR 2ND OR ADDITIONAL)(5W)S1
S9        373   S2 AND S8
S10        10   S3 AND S8
S11         6   S4 AND S8
S12         0   S5 AND S8
S13         0   S6 AND S8
S14        12   S7 AND S8
S15        24   S10:S14
S16        17   RD (unique items)
```

16/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06283714 E.I. No: EIP03057343174
Title: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions
Author: Micciancio, Daniele
Corporate Source: University of California, San Diego, La Jolla, CA 92093-0114, United States
Conference Title: The 34rd Annual IEEE Symposium on Foundations of Computer Science
Conference Location: Vancouver, BC, Canada Conference Date: 20021116-20021119
Sponsor: IEEE Computer Society TCMF
E.I. Conference No.: 60622
Source: Annual Symposium on Foundations of Computer Science - Proceedings 2002. p 356-365
Publication Year: 2002
CODEN: ASFPDV ISSN: 0272-5428
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0302W1
Abstract: We study a generalization of the compact knapsack problem for arbitrary rings: given m = O(log n) ring elements a//1, ..., a//m is a member of the set of R and a target value b is a member of the set of R, find coefficients x//1, ..., x//m is a member of the set of X (where X is a subset of R of size 2**n) such that Sigmaa//ix//i = b. The computational complexity of this problem depends on the choice of the ring R and set of coefficients X. This problem is known to be solvable in quasi polynomial time when R is the ring of the integers and X is the set of small integers left brace 0, ..., 2**n - 1 right brace . We show that if R is an appropriately chosen ring of modular polynomials and X is the subset of polynomials with small coefficients, then the compact knapsack problem is as hard to solve on the average as the worst case instance of approximating the covering radius (or the length of the shortest vector, or various **other** well known **lattice** problems) of any cyclic lattice within a polynomial factor. Our proof adapts, to the cyclic lattice setting, techniques initially developed by Ajtai for the case of general lattices. 34 Refs.
Descriptors: Optimization; Computational complexity; Algorithms; Set theory; Polynomials; **Cryptography** ; Security of data; Probability
Identifiers: Compact knapsack problem; Cyclic lattices; Worst-case average-case connection; One-way functions
Classification Codes:
921.5 (Optimization Techniques); 721.1 (Computer Theory (Includes Formal Logic, Automata Theory, Switching Theory & Programming Theory)); 723.1 (Computer Programming); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory); 921.1 (Algebra); 723.2 (Data Processing)
921 (Applied Mathematics); 721 (Computer Circuits & Logic Elements); 723 (Computer Software, Data Handling & Applications)
92 (ENGINEERING MATHEMATICS); 72 (COMPUTERS & DATA PROCESSING)

16/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05439381 E.I. No: EIP99124948500
Title: Linear phase paraunitary filter bank with filters of different lengths and its application in image compression
Author: Tran, Trac D.; Ikehara, Maasaki; Nguyen, Truong Q.
Corporate Source: Univ of Wisconsin, Madison, WI, USA
Source: IEEE Transactions on Signal Processing v 47 n 10 1999. p 2730-2744
Publication Year: 1999
CODEN: ITPRED ISSN: 1053-587X
Language: English

Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0002W1
Abstract: In this paper, the theory, structure, design, and implementation of a new class of linear-phase paraunitary filter banks (LPPUFB's) are investigated. The novel filter banks with filters of different lengths can be viewed as the generalized lapped orthogonal transforms (GenLOT's) with variable-length basis functions. Our main motivation is the application in block-transform-based image coding. Besides having all of the attractive properties of other lapped orthogonal transforms, the new transform takes advantage of its **long** , overlapping **basis** functions to represent smooth signals in order to reduce blocking artifacts, whereas it reserves **short** **basis** functions for high-frequency signal components like edges and texture, thereby limiting ringing artifacts. Two design methods are presented, each with its own set of advantages: The first is based on a direct lattice factorization, and the **second** enforces certain relationships between the **lattice** coefficients to obtain variable length filters. Various necessary conditions for the existence of meaningful solutions are derived and discussed in both cases. Finally, several design and image coding examples are presented to confirm the validity of the theory. (Author abstract) 23 Refs.
Descriptors: *Signal filtering and prediction; Image compression; Electric network synthesis; Electric network analysis; Mathematical transformations; Functions; Image coding; Image enhancement
Identifiers: Linear phase paraunitary filter banks; Generalized lapped orthogonal transforms
Classification Codes:
703.2.2 (Electric Filter Synthesis); 703.2.1 (Electric Filter Analysis)
716.1 (Information & Communication Theory); 723.2 (Data Processing); 703.2 (Electric Filters); 921.3 (Mathematical Transformations)
716 (Radar, Radio & TV Electronic Equipment); 741 (Optics & Optical Devices); 723 (Computer Software); 703 (Electric Circuits); 921 (Applied Mathematics)
71 (ELECTRONICS & COMMUNICATIONS); 74 (OPTICAL TECHNOLOGY); 72 (COMPUTERS & DATA PROCESSING); 70 (ELECTRICAL ENGINEERING); 92 (ENGINEERING MATHEMATICS)

16/5/3 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01804764 ORDER NO: AADAA-I9943358
AVERAGE-CASE VERSUS WORST-CASE COMPLEXITY OF COMPUTATION (LATTICES)
Author: NERURKAR, AJAY P.
Degree: PH.D.
Year: 1999
Corporate Source/Institution: STATE UNIVERSITY OF NEW YORK AT BUFFALO (0656)
Major Professor: JIN-YI CAI
Source: VOLUME 60/08-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 4060. 134 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

Two natural notions of hardness of computational problems are <italic>worst-case hardness</italic> which measures how hard the hardest instance of a problem is, and <italic>average-case hardness</italic> which is a measure of how hard it is to solve a randomly given instance. While the former is the more traditional notion, it might be argued that it is the latter that truly captures the complexity of the problem. From a **cryptographic** viewpoint too, it is the average-case complexity that is important.

This dissertation studies the connection between the two notions of complexity for specific problems, particularly ones involving <italic>lattices</italic>. The most important such problem is the Shortest Vector Problem (SVP): Given a lattice, compute a shortest non-zero vector in it. We improve upon a result of Miklós Ajtai who proved that the average-case hardness of this problem over a certain class of lattices was

equivalent to the worst-case hardness of **other lattice** problems. Since these latter problems are thought to be hard in the worst-case, this says that the SVP on that class is hard on average. This is significant for the security of a future **cryptosystem** based on the SVP. We also present a worst-case hardness result for the SVP, proving that it is NP-hard to find an approximately short vector in a given lattice.

A graph-theoretic application of lattices is also shown. The graphs considered are called <italic>circulant graphs</italic> and the problem is to find a shortest loop in such a graph. With every circulant graph is associated a lattice and finding a shortest loop in the graph is the same as finding a shortest vector in the lattice. This enables us to apply lattice techniques to study the complexity of this problem.

Finally, moving away from lattices, we show that a <italic>hierarchy </italic> exists for a probabilistic complexity class under certain hardness assumptions. The assumptions are worst-case, but for a hierarchy theorem to be proved, average-case hardness is required. We make use of standard techniques to effect the conversion. This once again underlines the usefulness of a connection between these two kinds of computational complexity.

16/5/4 (Item 2 from file: 35)

In 3970 ORDER NO: AAD98-04999

DEGREES OF GROBNER BASES OF INTEGER PROGRAMS

Author: HOSTEN, SERKAN
Degree: PH.D.
Year: 1997
Corporate Source/Institution: CORNELL UNIVERSITY (0058)

Source: VOLUME 58/08-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 4429. 102 PAGES
Descriptors: OPERATIONS RESEARCH
Descriptor Codes: 0796

This thesis is about the complexity of Grobner bases of integer programs. Given the family of integer programs$${\rm minimize}\ cx:Ax=b,\quad x\in {\bf N}\sp{n}$$as the right-hand-side vector b varies, we study the associated toric ideal and its Grobner bases with respect to term orders induced by the cost vector c. In Chapter 2 we discuss possible ways of bounding the degrees of reduced Grobner basis elements of toric ideals. The size of these elements is an important complexity measure in commutative algebra and algebraic geometry as well as integer programming. We develop two techniques to improve the existing bounds for the reduced Grobner basis elements. One of them relies on giving bounds on the Hilbert basis elements of certain polyhedral cones, and the **other** one depends on counting **lattice** points in a lattice polytope.

Chapter 3 presents a connection between the group relaxation in integer programming and localizations of initial ideals of the associated toric ideal. We identify the integer programs in the above family which cannot be solved by the group relaxation as those programs which correspond to the embedded primes of the initial ideal. This correspondence gives an algorithm to compute reduced Grobner bases of toric ideals. This algorithm is different from Buchberger's algorithm. Furthermore, a certain covering of the standard monomials of the initial ideals gives a combinatorial definition for another complexity measure called arithmetic degree. We give tight bounds for arithmetic degrees of initial ideals of one-dimensional toric ideals.

In Chapter 4 we answer a question posed by Batyrev. The question is concerned with the number of primitive collections of certain polyhedral fans which correspond to smooth complete projective toric varieties. We provide an example where this number is exponential in the codimension of the associated toric variety. The same example gives a toric ideal which has a reduced Grobner basis with exponentially many elements even though the initial ideal is square-free.

In the final chapter we present GRIN, a software that we developed for computing Grobner bases of toric ideals. This implementation of

Buchberger's algorithm is tailored for the toric ideals. In particular, we show two different approaches to compute the Grobner basis of a toric ideal by making **short** , successive Grobner **basis** computations.

16/5/5 **(Item 1 from file: 2)**
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

5494813 INSPEC Abstract Number: A9706-6310-001
Title: Linear-response theory and lattice dynamics: a muffin-tin-orbital approach
Author(s): Savrasov, S.Y.
Author Affiliation: Max-Planck-Inst. fur Festkorperforschung, Stuttgart, Germany
Journal: Physical Review B (Condensed Matter) vol.54, no.23 p. 16470-86
Publisher: APS through AIP,
Publication Date: 15 Dec. 1996 Country of Publication: USA
CODEN: PRBMDO ISSN: 0163-1829
SICI: 0163-1829(19961215)54:23L.16470:LRTL;1-A
Material Identity Number: P279-97005
U.S. Copyright Clearance Center Code: 0163-1829/96/54(23)/16470(17)/$10
Document Number: S0163-1829(96)05348-9
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: A detailed description of a method for calculating static linear-response functions in the problem of lattice dynamics is presented. The method is based on density-functional theory and it uses linear muffin-tin orbitals as a basis for representing first-order corrections to the one-electron wave functions. This makes it possible to greatly facilitate the treatment of the materials with localized orbitals. We derive variationally accurate expressions for the dynamical matrix. We also show that **large** incomplete- **basis** -set corrections to the first-order changes in the wave functions exist and can be explicitly calculated. Some useful hints on the k-space integration for metals and the self-consistency problem at long wavelengths are also given. As a test application we calculate bulk phonon dispersions in Si and find good agreement between our results and experiments. As **another** application, we calculate **lattice** dynamics of the transition-metal carbide NbC. The theory reproduces the major anomalies found experimentally in its phonon dispersions. The theory also predicts an anomalous behavior of the lowest transverse acoustic mode along the (xi xi 0) direction. Most of the calculated frequencies agree within a few percent with those measured. (49 Refs)
Subfile: A
Descriptors: density functional theory; elemental semiconductors; muffin-tin potential; niobium compounds; phonon dispersion relations; silicon; wave functions
Identifiers: static linear-response functions; lattice dynamics; density-functional theory; linear muffin-tin orbitals; first-order corrections; one-electron wave functions; localized orbitals; k-space integration; metals; self-consistency; bulk phonon dispersions; transverse acoustic mode; Si; NbC
Class Codes: A6310 (General theory of lattice dynamics and crystal statistics); A6320D (Phonon states and bands, normal modes, and phonon dispersion)
Chemical Indexing:
Si el (Elements - 1)
NbC bin - Nb bin - C bin (Elements - 2)

16/5/6 **(Item 2 from file: 2)**
DIALOG(R)File 2:INSPEC

02798035 INSPEC Abstract Number: C87006274
Title: Some algorithmic problems on lattices

Author(s): Lovasz, L.
Author Affiliation: ELTE TTK Math. Inst., Budapest, Hungary
Conference Title: Theory of Algorithms p.323-37
Editor(s): Lovasz, L.; Szemeredi, E.
Publisher: North-Holland, Amsterdam, Netherlands
Publication Date: 1986 Country of Publication: Netherlands 430 pp.
ISBN: 0 444 87760 6
Conference Date: 16-21 July 1984 Conference Location: Pecs, Hungary
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: There are two kinds of algorithmic problems: firstly one, may solve various problems for lattices given by a **basis** (e.g. finding a **shortest** lattice vector); secondly one may try to find a basis in a lattice defined in some other way. In the paper the author concentrates on the **second** kind of **lattice** problem. Among others, he proves that in a lattice given by a separation oracle with some mild additional information, a basis can be found in polynomial time. (11 Refs)
Subfile: C
Descriptors: algorithm theory; graph theory
Identifiers: algorithmic problems; lattices; algorithmic problems; basis; separation oracle; polynomial time
Class Codes: C1160 (Combinatorial mathematics); C4240 (Programming and algorithm theory)

16/5/7 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1623241 NTIS Accession Number: DE92715417
Experimental validation of geochemical computer models
Nilsson, K. ; Skytte Jensen, B.
Risoe National Lab., Roskilde (Denmark). Environmental Science and Technology Dept.
Corp. Source Codes: 100628015; 9800727
Report No.: NEI-DK-674
1991 74p
Languages: English
Journal Announcement: GRAI9206; ERA9210
U.S. Sales Only. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A04/MF A01
Country of Publication: Denmark
Geochemical computer programs have found increasing use as modelling tools for prediction of the changes occurring when a complicated chemical system is subjected to chemical perturbations. The aim was to compare calculations directly with laboratory experiments, to validate the computer program used and its database with experimental results obtained under controlled conditions and in this way certify the usefulness of predictive modelling. Experimental results obtained by equilibrating solid CaCO(sub 3), MgCO(sub 3)(basic) and their mixture with different aqueous solutions given containing trace amounts of radioactive Europium as an indicator of adsorption phenomena are presented. In summary geochemical computer programs are useful in **deciphering** experimental data. The exact thermodynamic values to be ascribed to e.g. minerals are influenced by particle size, by content of impurities and of **other lattice** defects, which may amount for a 'correction' up to 0.5 kcal/mole. It was experienced that unless the sampling procedures and laboratory practice are known for field data, the interpretation of comparative calculations shall be done with some hesitation. It is important not to neglect the possibility for long term changes in adsorption characteristics due to the formation of new surface phases. It was found that the original Davies equation served better in the interpretation of experimental data than the now recommended form and that for higher salt concentrations the decrease in the activity of water has to be taken into account. (AB).
Descriptors: *Geochemistry; Bench-Scale Experiments; Computer

Calculations; Forecasting; Petroleum Geology; Validation
Identifiers: *Foreign technology; *Computerized simulation; EDB/020200; NTISDEE
Section Headings: 48F (Natural Resources and Earth Sciences--Geology and Geophysics)

16/5/8 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

15267927 PASCAL No.: 01-0438006
Physiochemical aspects of tubulin-interacting antimitotic drugs
CORREIA J J; LOBERT S
Department of Biochemistry, University of Mississippi Medical Center, Jackson, MS 39216, United States; School of Nursing, University of Mississippi Medical Center, Jackson, MS 39216, United States
Journal: Current pharmaceutical design, 2001, 7 (13) 1213-1228
ISSN: 1381-6128 Availability: INIST-26320; 354000096106850030
No. of Refs.: 122 ref.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: Netherlands
Language: English
250 words): A diverse group of natural biological compounds bind to microtubules and suppress microtubule dynamics. Here we review the mechanism of microtubule assembly and dynamics as well as structural features that are important for nucleotide binding, GTP hydrolysis and stabilization of longitudinal and lateral protofilament contacts. Specific emphasis is placed upon the polar structure of the microtubule, the exposure of the nucleotide hydrolysis site at the + end and the conformational and configurational plasticity of the microtubule lattice. These features have important implications for the mechanism of dynamic instability and the disruptive action of antimitotic drugs. We then discuss the various classes of tubulin binding drugs emphasizing their site and mode of binding as well as the structural and energetic basis for their effects on microtubule assembly and dynamics. A common feature of tubulin-interacting compounds is a linkage to assembly, either the stabilization of a microtubule lattice by compounds like taxol or epothilone A, or the preferential formation of **alternate lattice** contacts and polymers at microtubule ends by compounds like colchicine, vinca alkaloids and **cryptophycin** -52. Finally, we explore the likely possibility that these drugs also disrupt the regulation of microtubule dynamics. Future generations of these compounds may be selectively developed to directly target the proteins that regulate mitotic spindle dynamics.

English Descriptors: Paclitaxel; Review; Tubulin; Microtubule; Molecular interaction; Antimitotic; Antineoplastic agent; Mechanism of action; Molecular dynamics; Binding site; Taxane derivatives

French Descriptors: Colchicine; Paclitaxel; Article synthese; Tubuline; Microtubule; Interaction moleculaire; Antimitotique; Anticancereux; Mecanisme action; Dynamique moleculaire; Site fixation; Taxane derive

Classification Codes: 002B02R01

16/5/9 (Item 1 from file: 434)
DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

05714806 Genuine Article#: SL583 Number of References: 41
Title: MONTE-CARLO RENORMALIZATION-GROUP CALCULATIONS OF CRITICAL BEHAVIOR IN THE SIMPLE-CUBIC ISING-MODEL
Author(s): PAWLEY GS; SWENDSEN RH; WALLACE DJ; WILSON KG
Corporate Source: UNIV EDINBURGH,DEPT PHYS/EDINBURGH EH9

3JZ/MIDLOTHIAN/SCOTLAND/; IBM CORP,RES LAB/CH-8803 RUSCHLIKON//SWITZERLAND/; CORNELL UNIV,NUCL STUDIES LAB/ITHACA//NY/14853
Journal: PHYSICAL REVIEW B-CONDENSED MATTER, 1984, V29, N7, P4030-4040
Language: ENGLISH Document Type: ARTICLE
Geographic Location: SCOTLAND; SWITZERLAND; USA
Subfile: SciSearch; CC PHYS--Current Contents, Physical, Chemical & Earth Sciences
Journal Subject Category: PHYSICS, CONDENSED MATTER
Research Fronts: 84-0748 001 (ISING-MODEL AND OTHER MODELS OF CRITICAL PHENOMENA IN FINITE-SIZE SCALING)
84-1752 001 (LATTICE GAUGE-THEORIES, MONTE-CARLO METHODS, CHIRAL-SYMMETRY, RENORMALIZATION-GROUPS AND FINITE-TEMPERATURE QCD)
84-1870 001 (APPLICATIONS AND COMPUTER ARCHITECTURE OF SYSTEMS USING PARALLEL ALGORITHMS AND PARALLEL PROCESSING MACHINES)
84-7087 001 (FACTORING ALGORITHMS FOR NUMBERS AND POLYNOMIALS, PRIMALITY TESTING AND **ENCRYPTION**)
84-8212 002 (CRITICAL BEHAVIOR AND RENORMALIZATION THEORIES OF DIRECTED AND **OTHER** SELF-AVOIDING WALKS ON **LATTICES** AND UNIVERSALITY OF LATTICES)
Cited References:

ADLER J, 1983, V16, P3585, J PHYS A
ADLER J, 1982, V26, P3958, PHYS REV B
AHLERS G, 1982, P1, PHASE TRANSITIONS CA
AMIT DJ, 1978, FIELD THEORY RENORMA
BAKER GA, 1978, V17, P1365, PHYS REV B
BAKER GA, 1976, V36, P1351, PHYS REV LETT
BELL TL, 1974, V10, P3935, PHYS REV B
BEYSENS D, 1982, P25, PHASE TRANSITIONS
BINDER K, V2, MONTE CARLO METHODS
BINDER K, 1981, V47, P693, PHYS REV LETT
BINDER K, 1981, V43, P119, Z PHYS B CON MAT Q
BOWLER KC, 1984, V72, P42, P IEEE
CHEN JH, 1982, V48, P630, PHYS REV LETT
CREUTZ M, 1983, V50, P1411, PHYS REV LETT
FREEDMAN BA, 1983, V15, L715 J PHYS A
GAUNT DS, COMMUNICATION
GAUNT DS, 1982, P217, PHASE TRANSITIONS CA
HAMER CJ, 1983, V16, P1257, J PHYS A
HOCKNEY RW, 1981, PARALLEL COMPUTERS
KNUTH DE, 1981, V2, ART COMPUTER PROGRAM
KOGUT J, 1974, V12, P76, PHYS REP C
LEGUILLOU JC, 1980, V21, P3976, PHYS REV B
LEGUILLOU JC, 1977, V39, P95, PHYS REV LETT
MA SK, 1976, V37, P471, PHYS REV LETT
MOLDOVER MR, 1982, P63, PHASE TRANSITIONS CA
NICKEL BG, 1982, P291, PHASE TRANSITIONS CA
PAWLEY GS, 1982, V47, P165, J COMPUT PHYS
PEARSON R, UNPUB PHYS REP
SENGERS JV, 1982, P95, PHASE TRANSITIONS CA
SMITH K, UNPUB
STAUFFER D, UNPUB
SWENDSEN RH, 1982, P57, REAL SPACE RENORMALI
SWENDSEN RH, UNPUB
WALLACE DJ, UNPUB PHYS REP
WALLACE DJ, 1983, P273, 6TH P J HOPK WORKSH
WEGNER FJ, 1976, V6, P34, PHASE TRANSITIONS CR
WILSON KG, 1975, V47, P773, REV MOD PHYS
WILSON KG, UNPUB
ZINJUSTIN J, COMMUNICATION
ZINJUSTIN J, 1981, V42, P783, J PHYS PARIS
ZINNJUSTIN J, 1982, P349, PHASE TRANSITIONS

16/5/10 (Item 1 from file: 266)
DIALOG(R)File 266:FEDRIP

00185683
IDENTIFYING NO.: 0245250 AGENCY CODE: NSF
Topics in Algebraic Geometry
PRINCIPAL INVESTIGATOR: Dolgachev, Igor V
PERFORMING ORG.: University of Michigan Ann Arbor, Mathematics, Ann Arbor , MI 48109-1109
PROJECT MONITOR: Mann, Benjamin M.
SPONSORING ORG.: National Science Foundation, DMS, 4201 Wilson Boulevard , Arlington, Virginia 22230
DATES: 20030701 TO 20040630 FY : 2003 FUNDS: $90,514 (90000)
SUMMARY: An algebraic surface of type K3 is a 2-dimensional analog of an elliptic curve. It is characterized by the property that its tangent bundle is not trivial but the first Chern class is trivial. Its group of algebraic automorphisms is a discrete group sometimes infinite sometimes finite and its structure is closely related to the structure of the orthogonal group of the the Picard group of divisor classes equipped with the intersection product. The structure of the automorphism group of a complex K3 surface is well understood thanks to the availability of trascendental methods based on the study of the integration of a holomorphic 2-form on the surface over transcendental cycles. No such methods are available in the case when the characteristic of the ground field is positive. In the proposal the principal investigator outlines several new approaches to the study of automorphism groups of K3 surfaces over such fields. Some of them based on the study of possible automorphisms of finite order which will allow to compute the character of the group in its representation on l-adic cohomology. Other approaches use the relationship between the Picard lattice and the 24-dimensional Leech lattice. The principal investigator will also study some applications to coding theory and **cryptology** related to K3 surfaces over a finite field. The study of symmetries of mathematical structures is one of the most important and oldest problems in mathematics. A symmetry group of a Riemann surface or an algebraic curve is now well understood. Much less is known about symmetries of higher dimensional algebraic varieties. The principal inverstigator proposes such study for a class of algebraic surfaces known as K3 surfaces which are two-dimensional analogs of elliptic curves. The symmetry groups of K3 surfaces are related to symmetry of **other** objects, for example **lattices** in hyperbolic spaces and convex polyhedra. Many known abstract infinite and finite groups admit a beautiful realization as symmetry groups of K3 surfaces. Applications of symmetry groups of elliptic curves over finite fields to coding theory and **cryptology** is well known. It is expected that the knowledge of symmetry groups of K3 surfaces over finite field will find new applications to these theories.

16/5/11 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

00798839 E94050344230
The normalized second **moment of the binary** lattice **determined by a convolutional code**
(Das normalisierte zweite Moment des binaeren Gitters bestimmt durch einen Konvolutionscode)
Calderbank, AR; Fishburn, PC
AT&T Bell Lab., Murray Hill, USA
IEEE Transactions on Information Theory, v40, n1, pp166-174, 1994
Document type: journal article Language: English
Record type: Abstract
ISSN: 0018-9448

ABSTRACT:
The authors calculate the per-dimension mean squared error micro(S) of the two-state convolutional code C with generator matrix (1,1 + D), for the symmetric binary source S = (0,1), and for the uniform source S = (0,1). When S = (0,1), the quantity micro(S) is the second moment of the coset weight distribution, which gives the expected Hamming distance of a random binary sequence from the code. When S = (0,1), the quantity micro(S) is the second moment of the Voronoi region of the modulo 2 binary lattice

determined by C. The key observation is that a convolutional code with 2(exp v) states gives 2(exp v) approximations to a given source sequence, and these approximations do not differ very much. It is possible to calculate the steady state distribution for the differences in these path metrics, and hence, the second moment. In this paper the authors shall only give details for the convolutional code (1,1 + D), but the method applied to arbitrary codes. The authors also define the covering radius of a convolutional code, and calculate this quantity for the code (1,1 + D).

DESCRIPTORS: WEIGHTING FUNCTION; **CIPHERING -- ENCRYPTION** ; CONVOLUTIONAL CODE; INFORMATION THEORY; MARKOV CHAIN; RANDOM PROCESS
IDENTIFIERS: HAMMING DISTANZ; TRELLIS QUANTISIERUNG; Konvolutionscode

16/5/12 (Item 1 from file: 62)
DIALOG(R)File 62:SPIN(R)
(c) 2004 American Institute of Physics. All rts. reserv.

00718768
Linear-response theory and lattice dynamics: A muffin-tin-orbital approach
Savrasov, S. Y.
Max-Planck-Institut fuer Festkoerperforschung, Heisenbergstrasse 1, D-70569 Stuttgart, Germany
PHYS REV B; 54(23),16470-16486 (15 Dec. 1996) CODEN: PRBMD
Work Type: THEORETICAL
A detailed description of a method for calculating static linear-response functions in the problem of lattice dynamics is presented. The method is based on density-functional theory and it uses linear muffin-tin orbitals as a basis for representing first-order corrections to the one-electron wave functions. This makes it possible to greatly facilitate the treatment of the materials with localized orbitals. We derive variationally accurate expressions for the dynamical matrix. We also show that **large** incomplete- **basis** -set corrections to the first-order changes in the wave functions exist and can be explicitly calculated. Some useful hints on the k-space integration for metals and the self-consistency problem at long wavelengths are also given. As a test application we calculate bulk phonon dispersions in Si and find good agreement between our results and experiments. As **another** application, we calculate **lattice** dynamics of the transition-metal carbide NbC. The theory reproduces the major anomalies found experimentally in its phonon dispersions. The theory also predicts an anomalous behavior of the lowest transverse acoustic mode along the ((xi) (xi) 0) direction. Most of the calculated frequencies agree within a few percent with those measured. (Copyright) 1996 The American Physical Society.
PACS: *71.10.-w, 63.20.Dj, 77.90.+k
Descriptors: LATTICE DYNAMICS ; CALCULATION METHODS ; DENSITY FUNCTIONAL METHOD ; MUFFIN-TIN POTENTIAL ; WAVE FUNCTIONS ; PHONON SPECTRA ; DISPERSION RELATIONS ; NIOBIUM CARBIDES ; ANOMALOUS PROPERTIES ; PSEUDOPOTENTIAL ; FOURIER TRANSFORMATION

16/5/13 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci
(c) 2004 American Mathematical Society. All rts. reserv.

03309295 MR 2002i#81041
Reversible quantum teleportation in an optical lattice.
Quantum information and computation.
Santos, Luis (Institut fur Theoretische Physik, Universitat Hannover, D-30167 Hannover, Germany)
Bruss, Dagmar (Institut fur Theoretische Physik, Universitat Hannover, D-30167 Hannover, Germany)
Corporate Source Codes: D-HANN-TP; D-HANN-TP
J. Phys. A
Journal of Physics. A. Mathematical and General, 2001, 34, no. 35, 7003--7015. ISSN: 0305-4470 CODEN: JPHAC5
Language: English Summary Language: English

Document Type: Journal
Journal Announcement: 200203
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (18 lines)

Quantum teleportation consists of the transport of a quantum state from one physical system to another using a previously entangled state. The original teleportation protocol proposed by C. H. Bennett et al. [Phys. Rev. Lett. 70 (1993), no. 13, 1895--1899; MR 94a:81004] involves a measurement capable of discriminating between Bell states, and therefore it is irreversible due to the collapse of the quantum state after such a measurement. However, S. L. Braunstein [Phys. Rev. A 53 (1996), no. 3, 1900--1902] showed that quantum teleportation can be performed without any irreversible detection if the detector is considered as a quantum system, the state of which is not read out. In this paper, this method is implemented to teleport an unknown state of a neutral atom in an optical lattice to another atom in **another** part of the **lattice** . This proposal is based on the procedure proposed by D. Jaksch et al. [Phys. Rev. Lett. 82 (1999), no. 9, 1975--1978] to entangle neutral atoms in a controlled way by using cold collisions between them.

Reviewer: Cabello, Adan (E-SEVL-AP2)
Review Type: Signed review
Descriptors: *81P15 -Quantum theory-Axiomatics, foundations, philosophy-Quantum measurement theory ; 81P68 -Quantum theory-Axiomatics, foundations, philosophy-Quantum computation and quantum **cryptography** (See also 68Q05, 94A60)

16/5/14 (Item 2 from file: 239)
DIALOG(R)File 239:Mathsci

02330852 MR 93b#11084
Quinary code construction of the Leech lattice.
Ozeki, Michio (Department of Information Science, Faculty of Science, Bunkyo, Hirosaki, Aomori, 036, Japan)
Corporate Source Codes: J-HIROSS-I
Nihonkai Math. J.
Nihonkai Mathematical Journal, 1991, 2, no. 2, 155--167.
Language: English
Document Type: Journal
Journal Announcement: 9208
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: SHORT (4 lines)

A self-dual quinary code of length 24 is used to construct the Leech lattice. The proof is based on a study of the Lee weight enumerator of the code. The existence of **another** construction of the Leech **lattice** using (special) self-dual codes of length 24 over prime fields is conjectured.

Reviewer: Litsyn, Simon N. (Ramat-Aviv)
Review Type: Signed review
Descriptors: *11H31 -Number theory-Geometry of numbers (For applications in coding theory see 94B75)-Lattice packing and covering (See also 05B40, 52C15, 52C17) ; 11T71 -Number theory-Finite fields and commutative rings (number-theoretic aspects)-Algebraic coding theory; **cryptography** ; 94B27 -Information and communication, circuits-Theory of error-correcting codes-Geometric methods (including applications of algebraic geometry) (See also 11T71

16/5/15 (Item 3 from file: 239)
DIALOG(R)File 239:Mathsci

01392755 MR 52##13549
Partitioning bases of Boolean lattices.
Quackenbush, Robert W.
Reichel, Hans-Christian
Algebra Universalis
1975, 5, no. 1, 148.

Language: English
Document Type: Journal
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (12 lines)

Let $\scr A=(A,{\bf F})$ be a (universal) algebra having the meet-semi-lattice with zero $(A,\wedge,0)$ as a reduct. A partitioning base S of $\scr A$ is a subset of A such that (i) S generates $\scr A$, and (ii) if a,b are in S, then $a\wedge b\in\{0,a,b\}$. The main result of the paper is that a Boolean lattice, i.e., a bounded complemented distributive lattice, has a partitioning base if and only if it is countable. On the **other** hand, there are bounded distributive **lattices** and Boolean algebras (i.e., Boolean lattices to which complementation has been added as a fundamental operation) having partitioning **bases** of arbitrarily **large** cardinality.

Reviewer: Cignoli, R.
Review Type: Signed review
Descriptors: *06A35 -Order, lattices, ordered algebraic structures (See also 18B35)-Ordered sets-Distributive lattices, generalizations

16/5/16 (Item 4 from file: 239)
DIALOG(R)File 239:Mathsci

01290996 MR 45##74
On the foundations of combinatorial theory: Combinatorial geometries. Preliminary edition.
Crapo, Henry H.
Rota, Gian-Carlo
Publ: The M.I.T. Press, Cambridge, Mass.-London, 1970, iv+289 pp. (not consecutively paged) (39 figures)
Price: $10.00.
Language: English
Document Type: Book
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (121 lines)

Combinatorics is a widely studied branch of mathematics nowadays, enriched with a vast number of new results and still offering a great variety of open problems. One of the main difficulties in combinatorial research is the lack of systematic theory. The authors of this book consider combinatorial geometry as a discipline that may be able to play a unifying role in the further development of the whole combinatorial theory. In the present (preliminary) edition the authors attempt to give a brief survey of the recent state of combinatorial geometry. Apart from a few new results the investigations are mainly expository, centered around the following problems: axiomatics of combinatorial geometry, description of examples, maps between geometries, coordinatization theory, matching theory and the critical problem. The notion of combinatorial geometry (introduced in $\S$ 2) arises as a generalization of the geometry of point-sets in finite dimensional projective spaces. Let S be any set admitting a closure relation that is a function $A\rightarrow\overline A$ defined for all subsets $A\subseteq S$ such that $A\subseteq\overline A$ and that $A\subseteq\overline B$ implies $\overline A\subseteq\overline B$ for any two subsets A,B of S; S is then called a closure space. A closure relation on S has the exchange property if for any two elements $a,b\in S$ and any subset $A\subseteq S$, the relations $a\in\overline{A\cup b}$ and $a\not\in\overline A$ imply that $b\in\overline{A\cup a}$. A closure relation on S has finite basis if and only if any subset $A\subseteq S$ contains a finite subset $A\sb f\subseteq A$ such that $\overline A\sb f=\overline A$. A combinatorial geometry $G(S)$ is a closure space consisting of a set S and a closure relation with finite basis and the exchange property such that the empty set is closed and $\overline a=a$ for all elements $a\in S$. The study of combinatorial geometries is justified by the fact that a great variety of combinatorial structures are combinatorial geometries; some of them are subsets of projective geometries, while others are of completely different origin. Six classical examples of combinatorial geometries are described in $\S$ 3; furthermore, simplicial geometries are considered, with the idea of developing a new

approach to combinatorial topology (see $\S$ 6). The closed subsets, or flats of a combinatorial geometry $G(S)$ form a lattice $L(S)$; hence combinatorial geometries can be studied from a lattice theoretic point of view. The lattice $L(S)$ is called a geometric lattice and is characterized as a semimodular point lattice without infinite chains (a chain of a lattice is any linearly ordered subset of L). In a geometric lattice each flat x has a well-defined $\text{rank}\,r(x)$ equal to the length of any maximal chain from $\overline\varphi$ to x; the rank function satisfies the relation $r(x)+r(y)\geq r(x\wedge y)+r(x\vee y)$. Properties of the rank and **other** **lattice** theoretic tools for the investigation of geometries are investigated ($\S$ 2) together with the internal structure of geometries ($\S$ 4). Many of the results have converses that yield characterizations of certain geometries. Interesting characterizations of geometries are obtained from **cryptomorphic** versions of geometries (see $\S$ 5). (Two mathematical theories are **cryptomorphic** whenever the basic notions of each can be identified with concepts of the other in such a way that both theories admit the same propositions.) The Whitney rank function on a set ($\S$ 5, pp. 5.12--5.13) and its generalizations (the semimodular functions; see $\S$ 7) are applied to construct new examples of geometries. Maps between geometries are introduced ($\S$ 9) generalizing the notion of a linear transformation in vector spaces. The study of invariants of the categories is initiated. $\S$ 10 contains a fundamental result about single point extensions of geometries: Given a geometry $G(S)$ all geometries $G\sp \ast=G(S\cup s)$ are constructed having one additional point s such that the points of $G\sp \ast$ different from S form a geometry isomorphic to G. In $\S$ 11 orthogonality of geometries on finite sets is considered, following Whitney who introduced orthogonality in his applications of geometries in graph theory (the authors use the term orthogonality instead of duality---a term previously used in this connection). One of the most developed sections of combinatorial geometry is the representation (or coordinatization) of geometries, treated in $\S$ 15. The problem of representation can be interpreted in the following way: Given a geometry $G(S)$ on a set S, find a module M over an integral domain R, a set $S\sb 1$ of submodules of M generated by single elements, and a one-to-one map of S onto $S\sb 1$ inducing an isomorphism of the geometry $G(S)$ onto the set $S\sb 1$ in terms of ordinary linear dependence (for the notion of linear dependence see Part 2 of $\S$ 3). A method is established for representing certain geometries as function space geometries (function space geometries are defined in $\S$ 3). Finally, the authors consider two fields of problems that they intend to investigate in their future research: matching theory and the critical problem. Most of the ``minimax'' theorems of combinatorial theory (such as the marriage theorems, Dilworth's theorem, the max-cut min-flow theorem of Ford and Fulkerson) can be generalized to combinatorial geometries. These generalizations form the subject of the matching theory. Without giving details about the whole theory, the authors restrict themselves to a new proof of the following generalization of the classical marriage theorem of P. Hall and R. Rado ($\S$ 8): ``In a combinatorial geometry $G(S)$ on a set S consider n subsets $A\sb 1,\cdots,A\sb n$. A necessary and sufficient condition for the existence of an independent set of n distinct elements $(x\sb 1,\cdots,x\sb n)$ where $x\sb i\in A\sb i$, $i=1,\cdots,n$, is that $(A\sb {j\sb 1}\cup A\sb {j\sb 2}\cup\cdots\cup A\sb {j\sb k})\geq k$ for any subfamily $A\sb {j\sb 1},A\sb {j\sb 2},\cdots,A\sb {j\sb k}$ of the sets $A\sb i$. The critical problem is stated only for chain groups over finite fields (introduced in $\S$ 3): ``In the n-dimensional vector space $V\sb n$ over the Galois Field $\text{GF}(q)$ let S be any subset of points not containing the origin. Find the minimal number c of projective hyperplanes $H\sb 1,\cdots,H\sb k$ such that the intersection $H\sb 1\cap H\sb 2\cap\cdots\cap H\sb c\cap S$ is the empty set.'' ($\S$ 16) The connection between the critical problem and the problem of coloring of graphs is explained. The authors believe that the critical problem provides a new ``setting'' for the study of the coloring problem with the required level of natural generality ($\S$ 1). In their opinion a systematic study of the critical problem should start with problems much simpler than the coloring problem. They hope that in this way techniques can be developed that may lead to solutions of general problems. The book is supplied with a detailed bibliography on the subject. There are some misprints in this preliminary version of the text.

Reviewer: Cofman, J.
Review Type: Signed review
Descriptors: *05-02 -Combinatorics (For finite fields, see 11Txx)-
Research exposition (monographs, survey articles)

16/5/17 **(Item 5 from file: 239)**
DIALOG(R)File 239:Mathsci

01095632 MR 20##2117
Kontinuumstheorie der Versetzungen und Eigenspannungen.
Kroner, Ekkehart
Publ: Springer-Verlag, Berlin-Gottingen-Heidelberg
1958, vii+179 pp.
Series: Ergebnisse der angewandten Mathematik. Bd. 5
Language: German
Document Type: Book
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (139 lines)

In 1934 Taylor explained the plastic deformation of metals on the basis of dislocation theory. A lot of work followed in both the macroscopic and microscopic fields. The present book treats dislocation theory from the continuum view point.

The continuum theory of dislocations has played an important role in bridging the gap between the phenomenological and atomic theories of plasticity. The author rightly says that this theory can be considered a significant contribution to scientific research in this century. The book follows the lines of R. Grammel's collection ``Verformung und Fliessen des Festkorpers'' [Springer, Berlin-Gottingen-Heidelberg, 1956; MR 19, 336], which treats both the mechanical and mathematical aspects, on the one hand, and the solid state physics aspect on the other.

The physical ideas of edge and screw dislocations, slip vector and glide planes, Burger's vector and the analogy between thermal (included here under the type called quasi-plastic) deformation and plastic deformation are explained, with figures, in the introduction.

The relations between the geometry of deformation and the dislocations is treated in the first chapter. After explaining the connection between Volterra's distortion and dislocations and proving that the lines of dislocation must either be closed loops or must end at the surfaces only, the author introduces the total (elastic and plastic) distortion tensor $(\overline\beta\sp T)$ as $ds\sb j{}\sp T=\beta\sb {ij}{}\sp Tdx\sb i$. Using the condition that connectivity of the body is preserved, it is shown that $\text{Rot}\,\overline\beta\sp T=0$. Defining dislocation density as $\overline\alpha=(\alpha\sb {ij})=-\text{Rot}\,\beta\sp p$ (where $\overline\beta\sp p$ is plastic component of $\overline\beta\sp T$), the basic geometric equation of continuum mechanics $\overline\alpha=\text{Rot}\,\overline\beta$ is deduced ($\overline\beta$ being the elastic component). Since it is the moving dislocations that cause slip and hence plastic flow, a tensor $N\sb {ijk}$ is introduced to represent the movement of $\alpha\sb {jk}$ dislocations in the i-direction, $j=k$ and $j\neq k$ giving screw and edge dislocations.

Then follows the decomposition of distortion into components as gradient and curl of two parts and further into the form $$ \nabla\sb iS\sb j{}'-\varepsilon\sb {ikl}\varepsilon\sb {jmn}\nabla\sb k\nabla\sb mi\sb {ln}+\theta\sb {ij}=\text{Grad}\,\overline s+\text{Ink}\,i+\overline\theta, $$ the compatibility conditions of classical theory being given by $\text{Ink}\,\overline\varepsilon=0$. The incompatible deformation fields arising in thermal and magnetic fields are then discussed. Finally we get discussions about structural rotations, large deformations and the determination of the distortion of a substance with dislocations.

The second chapter deals with the statical viewpoint. Volume and surface dislocations are treated. By use of the stress-function approach the energy of volume distributions is obtained and the particular case of two volume distributions is noted, giving self and mutual energies. Expanding the method of obtaining general solutions of classical elasticity theory (with anisotropy) the displacement fields for line and surface distributions are obtained. It is shown that a field arising from dislocations can be

considered, similar to the magnetic field, as due to either line distributions or surface distributions of dislocations. The case of singular dislocations is then discussed and from classical elasticity theory self and mutual energies are obtained, noting their analogy to self and mutual inductances. Finally, stress fields due to dislocations are treated. By use of the principle of virtual displacement the formula of Peach and Koehler $d\overline K=d\overline Lx\sp {\overline\sigma}\cdot\overline b$ is obtained, $d\overline K$ being force, $d\overline L$ displacement, $x\sp {\overline\sigma}$ stress and $\overline b$ Burger's vector. This is applied to obtain stress and displacement fields due to different types of multiple force and displacement singularities. Analogies with the electro-magnetic field are frequently noted.

We then get the discussion on dislocations in crystals. The basic concepts in the order of magnitude of infinitesimals involved in the mathematical treatment of the microscopic region and of the passage to the macroscopic are discussed. Starting with Frank's definition of dislocation in crystals, displacements, distortion and deformation in the microscopic are explained leading to $\delta\sb {\text{Rot}\,\overline\beta=\overline\alpha}$ as before, showing the existence of elastic distortion in presence of dislocations. With this the author passes to the macroscopic region and establishes relevant equations. Then the relations between the grain-boundary orientations and dislocation arrangements are discussed. The resulting relations giving the type and density of dislocations which give stresses or no stresses are deduced. Dislocation types in cubic face-centred crystals are then discussed. Finally Peierl's and Eshelby's treatments of edge and screw dislocations for primitive cubic crystals, and Liebfried and Dietze's treatment for face centred cubic crystals is given in detail.

The fourth chapter deals with the non-Riemannian geometry of dislocations. Kundo's and Bilby-Bullough-Smith's (B.B.S.) theories are first discussed.

Defining the Cartan's torsion tensor $(\Gamma\sp \kappa{}\sb {[\lambda\mu]})$, Riemann-Christoffel curvature tensor $(R\sp \kappa{}\sb {\lambda\mu\nu})$ and Euler-Schouten's curvature tensor $(H\sb {ij}{}\sp \Lambda)$, it is shown that the dislocation density can be related to torsion as $\alpha\sp {\lambda\kappa}=\varepsilon\sp {\lambda\mu\nu}\Gamma\sp \kappa{}\sb {[\mu\nu]}$. Then Kundo's classification of lattice flaws as (i) those with incompatible metric with non-vanishing curvature in natural state (points of curvature flaw) (ii) non-Riemannian lattice defects with non-vanishing torsion in natural state (points of torsion flaws) (iii) Lattice flaws with non-vanishing Euler-Schouten's curvature, and the agreement with the ideas in the book is then noted. The B.B.S. theory is then given. Starting with the geometry of deformation of lattices relations between the geometric quantities and local and true Burger's vector (identical only for small deformation), torsion tensor and dislocation density and curvature tensor and stress-free state are discussed. The relation between Nye's curvature tensor and torsion in non-Riemannian geometry is then explained. The chapter closes with a discussion of how Kundo's and B.B.S.'s theories pertain to the macroscopic and microscopic regions, respectively, how a new theory of plasticity can be built up from non-Riemannian geometry and the relations between the virtual (Kundo's), real and local densities of dislocations.

In the last chapter we have some applications.

The first one is the interesting but difficult problem of work-hardening of metals. Here we get an outline of the case of cubic face centred metals. The stress-strain curve is divided into 3 parts.

The small amount of hardening in the first region is easily explained. For the second region where hardening coefficient is **large** , it is explained on the **basis** of the occurrence of Lomer-Cotterell dislocations when a Frank-Read source of dislocation meets another on a different slip-plane. The case of small coefficient in the last region, it is noted, is still not solved satisfactorily. The explanation of `active energy' is given, and a method to calculate it.

The next application is to the approximate calculation of self-energy of curvilinear dislocations.

Then the notion of interstitial or foreign atoms acting as dipoles and

polarisation centres is explained. Interactions of these and other lattice faults with dislocations are treated mathematically.

```
File 348:EUROPEAN PATENTS 1978-2004/Feb W03
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040219,UT=20040212
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1      30847   LATTICE? ? OR LATICE? ?
S2     438140   BASES OR BASIS
S3      10136   S2(5N)(LONG??? OR LARGE??)
S4       6612   S2(5N)(SMALL??? OR SHORT???)
S5      49851   (DIGITAL? OR ELECTRONIC?)(3N)(SIGN OR SIGNS OR SIGNED OR S-
             IGNING OR SIGNER OR SIGNATURE? ?)
S6       6345   PUBLIC()KEY? ? OR (ASYMMETRIC? OR TWO(W)KEY? ?)(3N)(CRYPT?
             OR CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
              ENCOD? OR SCRAMBL?)
S7      42220   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
              ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
             OR UNSCRAMBL?
S8       1085   S1(50N)S2
S9         17   S1(50N)S3
S10         7   S1(50N)S4
S11      2030   (TWO OR DUAL? OR TWIN OR MULTIPL? OR PLURAL? OR DIFFERENT)-
             (5W)S1
S12        50   S11(50N)S2
S13        55   S1(50N)S5
S14         9   S1(50N)S6
S15        29   S1(50N)S7
S16        50   S9:S10 OR S14:S15
S17        49   S13 NOT S16
```

16/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01165276
A METHOD FOR ACCELERATING CRYPTOGRAPHIC OPERATIONS ON ELLIPTIC CURVES
VERFAHREN ZUR BESCHLEUNIGUNG KRYPTOGRAPHISCHER OPERATIONEN AUF ELLIPTISCHEN KURVEN
PROCEDE D'ACCELERATION DES OPERATIONS CRYPTOGRAPHIQUES SUR DES COURBES ELLIPTIQUES
PATENT ASSIGNEE:
Certicom Corp., (2118052), 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L4W 5L1, (CA), (Proprietor designated states: all)
INVENTOR:
GALLANT, Robert, 4788 Rosebush Road, Mississauga, Ontario L5M 5N1, (CA)
LAMBERT, Robert, J., 63 Holm Street, Cambridge, Ontario N3C 3N3, (CA)
VANSTONE, Scott, A., 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0, (CA)
LEGAL REPRESENTATIVE:
de Vries, Johannes Hendrik Fokke et al (46332), De Vries & Metman Overschiestraat 180, 1062 XK Amsterdam, (NL)
PATENT (CC, No, Kind, Date): EP 1141820 A1 011010 (Basic)
EP 1141820 B1 021106
WO 2000039668 000706
APPLICATION (CC, No, Date): EP 99962006 991223; WO 99CA1222 991223
PRIORITY (CC, No, Date): CA 2257008 981224
DESIGNATED STATES (Pub A): AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; (Pub B): CH; DE; FR; GB; LI
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-007/72
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200245	359
CLAIMS B	(German)	200245	389
CLAIMS B	(French)	200245	396
SPEC B	(English)	200245	4711
Total word count - document A			0
Total word count - document B			5855
Total word count - documents A + B			5855

...SPECIFICATION of achieving this solution is described below in greater detail.
To produce small ai)) and bi)), it is possible to make use of the L3)-**lattice** basis reduction algorithm (HAC p.118), which would directly result in **short basis** vectors. However, in this preferred embodiment the simple extended Euclidean algorithm is employed on the pair (n, (lambda)). The extended Euclidean algorithm on (n, (lambda...

16/3,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01056450
A method for authentification item
Ein Verfahren fur die Beglaubigung von Elementen
Un procede pour l'authentification d'elements
PATENT ASSIGNEE:
YEDA RESEARCH & DEVELOPMENT COMPANY, LTD., (268946), Weizman Institute of Science P.O. Box 95, 76100 Rehovot, (IL), (Applicant designated States: all)
INVENTOR:
Naor, Moni, 5 Beit-Zori Street, Tel Aviv 69122, (IL)
Nissim, Yaacov, 28 Haruzim Street, Ramat-Gan 52525, (IL)
LEGAL REPRESENTATIVE:

Joly, Jean-Jacques et al (39741), Cabinet Beau de Lomenie 158, rue de l'Universite, 75340 Paris Cedex 07, (FR)
PATENT (CC, No, Kind, Date): EP 932109 A2 990728 (Basic)
EP 932109 A3 030618
APPLICATION (CC, No, Date): EP 99400130 990121;
PRIORITY (CC, No, Date): US 10571 980122
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-017/30; H04L-009/32
ABSTRACT WORD COUNT: 106
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9930	531
SPEC A	(English)	9930	6284
Total word count - document A			6815
Total word count - document B			0
Total word count - documents A + B			6815

...SPECIFICATION IEEE Symp. on Foundations of Computer Science, pp. 540-545,

1989.
(6) M. Bellare, P.Rogaway. "Collision-Resistant Hashing: Towards Making UOWHFs Practical". Advances in **Cryptology** - **CRYPTO** '97, Lecture Notes in Computer Science, Springer-Verlag, 1997.
(11) S. Even, O. Goldreich, S. Micali. "On-Line/Off-Line Digital Signatures". Journal of **Cryptology** , Springer-Verlag, Vol. 9 pp. 35-67, 1996.
(12) O. Goldreich, S. Goldwasser, and S. Halevi,. "Collision-Free Hashing from **Lattice** Problems". ECCC, TR96-042, 1996.

http: //www. eccc. unitrier. de/eccc/
(13) A. Herzberg, H. Yochai. "Mini-Pay: Charging per Click on the Web". Proc...

16/3,K/8 **(Item 8 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00674614
Encoder using the tunnel current effect
Tunnelstromkodierer
Codeur utilisant les courants a effet tunnel
PATENT ASSIGNEE:
CANON KABUSHIKI KAISHA, (542361), 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP), (applicant designated states: BE;CH;DE;FR;GB;IT;LI;NL;SE)
INVENTOR:
Yanagisawa, Yoshihiro, c/o Canon Kabushiki Kaisha 3-30-2,Shimomaruko,, Ohta-ku, Tokyo, (JP)
Morikawa, Yuko, 231-7 Kamihirama, Nakahara-ku, Kawasaki-shi, Kanagawa-ken , (JP)
Matsuda, Hiroshi, 1252-3 Takamori, Isehara-shi, Kanagawa-ken, (JP)
Kawada, Haruki, c/o Canon Kabushiki Kaisha 3-30-2,Shimomaruko, Ohta-ku, Tokyo, (JP)
Sakai, Kunihiro, 301, Shimizu-manshion, 1385-1 Ishida, Isehara-shi, Kanagawa-ken, (JP)
Kawade, Hisaaki, c/o Canon Kabushiki Kaisha 3-30-2,shimomaruko, Ohta-ku, Tokyo, (JP)
Eguchi, Ken, 1-15-H-302 Higashiterao, Tsurumi-ku, Yokohama-shi, Kanagawa-ken, (JP)
Murakami, Eigo, 202, Copo-Kato, 337 Kamigo, Ebina-shi, Kanagawa-ken, (JP)
[illegible], Toshimitsu, c/o Canon Kabushiki Kaisha, 3-30-2 Shimomaruko,

Ohta-ku, Tokyo, (JP)
Yoshii, Minoru, 1-14-24, Higashinakano, Nakano-ku, Tokyo, (JP)
Saitoh, Kenji, c/o Canon Kabushiki Kaisha 3-30-2,Shimomaruko, Ohta-ku, Tokyo, (JP)
Yamano,Akihiko, c/o Canon Kabushiki Kaisha 3-30-2,Shimomaruko, Ohta-ku, Tokyo, (JP)
Nose, Hiroyasu, 3-4731-1-204 Sobudai, Zama-shi, Kanagawa-ken, (JP)
LEGAL REPRESENTATIVE:
Hellmann, Hans-Bernd, Dipl.-Ing. et al (9227), Patentanwaltsburo Tiedtke-Buhling-Kinne & Partner Bavariaring 4, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 646913 A2 950405 (Basic)
EP 646913 A3 960821
EP 646913 B1 990113
APPLICATION (CC, No, Date): EP 94120561 880824;
PRIORITY (CC, No, Date): JP 87212153 870825; JP 87212154 870825; JP 87305747 871204; JP 87305748 871204; JP 87309421 871209; JP 88201306 880812; JP 88201307 880812; JP 88201308 880812
DESIGNATED STATES: BE; CH; DE; FR; GB; IT; LI; NL; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 304893 (EP 881137947)
INTERNATIONAL PATENT CLASS: G11B-009/00; G01N-027/00; G01B-007/00;
ABSTRACT WORD COUNT: 197

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9902	232
CLAIMS B	(German)	9902	232
CLAIMS B	(French)	9902	280
SPEC B	(English)	9902	29087
Total word count - document A			0
Total word count - document B			29831
Total word count - documents A + B			29831

...SPECIFICATION present invention wherein non-periodic graduations are used as a reference scale.
Figure 11 is a schematic and diagrammatic view showing the structure of an **encoder** wherein an **asymmetric** -shape reference scale is used as a reference scale.
Figure 12 is a waveform view showing signals which are obtainable in the explanatory embodiment of Figure 11.
Figures 13A and 13B are schematic views showing a plane (1,1,1) of a face-centered cubic **lattice** , which is a specific explanatory example of an asymmetric reference scale, wherein Figure 13A is a top plan view and Figure 13B is a sectional...

16/3,K/9 **(Item 9 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00503361
NON-LINEAR OPTICAL DEVICE
NICHT-LINEARE, OPTISCHE VORRICHTUNG
DISPOSITIF OPTIQUE NON LINEAIRE
PATENT ASSIGNEE:
SECRETARY OF STATE FOR DEFENCE IN HER BRITANNIC MAJESTY'S GOV. OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, (201674), Whitehall, London SW1A 2HB, (GB), (applicant designated states: AT;BE;DE;DK;FR;GB;IT;LU;NL;SE)
INVENTOR:
SKEDDON, Kenneth, Richard Upper St. Mary's Mead, Broadhill, Oakley Lane Keymer West Sussex BN6 8PA, (GB)
AAKEROY, Christer, Bjorn Elat 2, 81 Montpelier Road, Brighton West Sussex BN1 3BD, (GB)
BLAGDEN, Nicholas 214 Pensby Road Heswall, Wirral, Merseyside LS1 6UF, (GB)
PATELL, Yasmin 171 Riverdale Road, Erith, Kent DA8 1PY, (GB)

LEGAL REPRESENTATIVE:
  Beckham, Robert William et al (28161), Defence Research Agency
    Intellectual Property Department DRA Farnborough, Farnborough, Hants.
    GU14 6TD, (GB)
PATENT (CC, No, Kind, Date): EP 526486 A1 930210 (Basic)
                             EP 526486 B1 960731
                             WO 9116657 911031
APPLICATION (CC, No, Date): EP 91907720 910419; WO 91GB616 910419
PRIORITY (CC, No, Date): GB 9008878 900420
DESIGNATED STATES: AT; BE; DE; DK; FR; GB; IT; LU; NL; SE
INTERNATIONAL PATENT CLASS: G02F-001/35;
NOTE:
  No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
      CLAIMS B (English) EPAB96 265
      CLAIMS B (German) EPAB96 236
      CLAIMS B (French) EPAB96 301
      SPEC B (English) EPAB96 4793
Total word count - document A 0
Total word count - document B 5595
Total word count - documents A + B 5595

...SPECIFICATION Examples of such organic bases include optionally substituted bases selected from piperidine, pyridine, piperazine, benzylamine, imidazole, pyrimidine and phenylethylamine.
  One preferred class of organic nitrogenous **bases** are compounds which possess **large** secondary molecular susceptibilities and as a result can exhibit SHG responses of large magnitude at certain molecular alignments within a crystal **lattice** . These compounds, which preferably have secondary molecular susceptibilities (beta-values) greater than 1 x 10(sup(-30) esu, more preferably greater than 10 x 10...

16/3,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00401090
Mapping digital data sequences for data transmission
Abbildung von digitalen Datenfolgen fur die Datenubertragung
Attribution de sequences de donnees numeriques pour la transmission de donnees
PATENT ASSIGNEE:
  MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
  Eyuboglu, Vedat M., 566 Commonwealth Avenue, No. 1005, Boston, MA 02215, (US)
  Forney, G. David, Jnr., 6 Coolidge Hill Road, Cambridge, MA 02138, (US)
LEGAL REPRESENTATIVE:
  Deans, Michael John Percy et al (30021), Lloyd Wise, Tregear & Co., Commonwealth House, 1-19 New Oxford Street, London WC1A 1LW, (GB)
PATENT (CC, No, Kind, Date): EP 397537 A2 901114 (Basic)
                             EP 397537 A3 920805
                             EP 397537 B1 970115
APPLICATION (CC, No, Date): EP 90305173 900514;
PRIORITY (CC, No, Date): US 351186 890512
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: H04L-027/00; H04L-025/497;
ABSTRACT WORD COUNT: 87

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
      CLAIMS A (English) EPABF1 1399

CLAIMS B	(English)	EPAB97	1419
CLAIMS B	(German)	EPAB97	1297
CLAIMS B	(French)	EPAB97	1703
SPEC A	(English)	EPABF1	10848
SPEC B	(English)	EPAB97	10287

Total word count - document A 12248
Total word count - document B 14706
Total word count - documents A + B 26954

...IFICATION bauds). Note that a fundamental region of the time-zero ...ttice RZ4) will contain exactly 22x6.5+1) points from any coset of the ...aled **lattice** 2-3)Z4); i.e., (vertical bar)2-3)Z4)/RZ4)(vertical bar)=214).

A small buffer 130 is filled with bits received from the DTE at the rate of 6.5 bits per (2D) signaling interval. In successive bauds, a **scrambler** 132 alternates in taking 7 or 6 bits from this buffer. The scrambled bits are delivered to a binary encoder in groups of 13 so...

16/3,K/13 (Item 13 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00297246

Encoder.
Codiereinrichtung.
Codeur.

PATENT ASSIGNEE:
CANON KABUSHIKI KAISHA, (542361), 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP), (applicant designated states: BE;CH;DE;FR;GB;IT;LI;NL;SE)

INVENTOR:
Yanagisawa, Yoshihiro, Canon-ryo 2-6-29 Mizuhiki Atsugi-shi, Kanagawa-ken, (JP)
Morikawa, Yuko, 231-7 Kamihirama Nakahara-ku, Kawasaki-shi Kanagawa-ken, (JP)
Matsuda, Hiroshi, 1252-3 Takamori, Isehara-shi Kanagawa-ken, (JP)
Kawada, Haruki, 48-1-1-208 Kamadai Hodogaya-ku, Yokohama-shi Kanagawa-ken, (JP)
Sakai, Kunihiro, 301, Shimizu-manshion 1385-1 Ishida, Isehara-shi Kanagawa-ken, (JP)
Kawade, Hisaaki, Canon-ryo 2-6-29 Mizuhiki Atsugi-shi, Kanagawa-ken, (JP)
Eguchi, Ken, 1-15-H-302 Higashiterao Tsurumi-ku, Yokohama-shi Kanagawa-ken, (JP)
Kawakami, Eigo, 202, Copo-Kato 337 Kamigo, Ebina-shi, Kanagawa-ken, (JP)
Kawase, Toshimitsu, Canon-ryo 2-6-29 Mizuhiki Atsugi-shi, Kanagawa-ken, (JP)
Yoshii, Minoru, 1-14-24 Higashinakano, Nakano-ku Tokyo, (JP)
Saitoh, Kenji, 1-30-40-132 Higashiterao Tsurumi-ku, Yokohama-shi Kanagawa-ken, (JP)
Yamano, Akihiko, 16-7 Tsutsujigaoka Midori-ku, Yokohama-shi Kanagawa-ken, (JP)
Nose, Hiroyasu, 3-4731-1-204 Sobudai, Zama-shi Kanagawa-ken, (JP)

LEGAL REPRESENTATIVE:
Tiedtke, Harro, Dipl.-Ing. et al (11949), Patentanwaltsburo Tiedtke-Buhling-Kinne & Partner Bavariaring 4, D-80336 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 304893 A2 890301 (Basic)
EP 304893 A3 930407
EP 304893 B1 950719
APPLICATION (CC, No, Date): EP 88113794 880824;
PRIORITY (CC, No, Date): JP 87212153 870825; JP 87212154 870825; JP 87305747 871204; JP 87305748 871204; JP 87309421 871209; JP 88201306 880812; JP 88201307 880812; JP 88201308 880812
DESIGNATED STATES: BE; CH; DE; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: G11B-009/00; G01N-027/00; G01D-005/244; H03M-001/00;
ABSTRACT WORD COUNT: 174

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	865
CLAIMS B	(English)	EPAB95	964
CLAIMS B	(German)	EPAB95	911
CLAIMS B	(French)	EPAB95	1098
SPEC A	(English)	EPABF1	29444
SPEC B	(English)	EPAB95	29389
Total word count - document A			30313
Total word count - document B			32362
Total word count - documents A + B			62675

...SPECIFICATION an example wherein non-periodic graduations are used as a reference scale.

Figure 11 is a schematic and diagrammatic view showing the structure of an **encoder** wherein an **asymmetric** -shape reference scale is used as a reference scale.

Figure 12 is a waveform view showing signals which are obtainable in the embodiment of Figure 11.

Figures 13A and 13B are schematic views showing a plane (1,1,1) of a face-centered cubic **lattice** , which is a specific example of an asymmetric reference scale, wherein Figure 13A is a top plan view and Figure 13B is a sectional view...

...SPECIFICATION an example wherein non-periodic graduations are used as a reference scale.

Figure 11 is a schematic and diagrammatic view showing the structure of an **encoder** wherein an **asymmetric** -shape reference scale is used as a reference scale.

Figure 12 is a waveform view showing signals which are obtainable in the embodiment of Figure 11.

Figures 13A and 13B are schematic views showing a plane (1,1,1) of a face-centered cubic **lattice** , which is a specific example of an asymmetric reference scale, wherein Figure 13A is a top plan view and Figure 13B is a sectional view...

16/3,K/16 (Item 16 from file: 348)

00145816

Television scrambling and descrambling method and apparatus.
Verfahren und Apparat zur Fernsehverschleierung und -entschleierung.
Procede et appareil pour embrouillage et desembrouillage de television.

PATENT ASSIGNEE:
R F MONOLITHICS, INC., (327970), 4441 Sigma Road, Dallas, TX 75234, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Ragan, Lawrence H. c/o R.F. Monolithics, Inc., 4441 Sigma Road, Dallas Texas 75234, (US)
Hartmann, Clinton S. c/o R.F. Monolithics, Inc., 4441 Sigma Road, Dallas Texas 75234, (US)
Ash, Darrell L. c/o R.F. Monolithics, Inc., 4441 Sigma Road, Dallas Texas 75234, (US)
LEGAL REPRESENTATIVE:
Brunner, Michael John et al (28871), GILL JENNINGS & EVERY 53-64 Chancery Lane, London WC2A 1HN, (GB)

PATENT (CC, No, Kind, Date): EP 140705 A2 850508 (Basic)
EP 140705 A3 870902
EP 140705 B1 920408
APPLICATION (CC, No, Date): EP 84307470 841030;
PRIORITY (CC, No, Date): US 547070 831031; US 547027 831031; US 547413 831031
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04N-007/16;
ABSTRACT WORD COUNT: 154

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	1500
CLAIMS B	(German)	EPBBF1	1491
CLAIMS B	(French)	EPBBF1	1764
SPEC B	(English)	EPBBF1	7729
Total word count - document A			0
Total word count - document B			12484
Total word count - documents A + B			12484

...SPECIFICATION It can also be constructed in a number of well known ways, but preferably consists of variable coils and/or capacitors in a ladder or **lattice** network, in a manner well known in the art. Thus, both amplitude and phase can be adjusted by the user of the descrambler during a period prior to the occurrence of the event or programme. A test pattern is transmitted with a one or two colour constant signal **scrambled** with a fixed, switch pattern in each frame. The amplitude is adjusted with the attenuator adjustment 92 to eliminate any "venetian blind" effect on the...

16/3,K/17 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01052380
CODE, DEVICE AND METHOD
CODE, DISPOSITIF ET PROCEDE
Patent Applicant/Inventor:
KOZICA Marcus, Hjarnegatan 4, 3tr. og, S-112 29 Stockholm, SE, SE (Residence), SE (Nationality)
GUSTAVSSON Vilhelm, Skeppargatan 100, 4 tr, S-115 30 Stockholm, SE, SE (Residence), SE (Nationality)
Legal Representative:
FALK Christer (et al) (agent), Zacco Sweden AB, Box 23101, S-104 35 Stockholm, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200381502 A2 20031002 (WO 0381502)
Application: WO 2003SE505 20030326 (PCT/WO SE0300505)
Priority Application: SE 2002948 20020326; US 2002162206 20020605
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9565

Fulltext Availability:
Detailed Description

Detailed Description
... sequence in accordance to one embodiment of the present invention is exemplified in Table 9 with reference to Table 10. The use of compression or **encryption** has not been yet decided in this example.

The code sequence can alternatively be distributed in a 2-dimensional grid or in a 3dimensional **lattice** .

The decoding device is, according to an embodiment of the invention, constituted of a decoding software program, or an algorithm for modulo arithmetic decoding. Alternatively...

16/3,K/18 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

[illegible] **Image available**
DIGITAL SIGNATURE AND AUTHENTICATION METHOD AND APPARATUS
SIGNATURE NUMERIQUE ET PROCEDE ET DISPOSITIF D'AUTHENTIFICATION
Patent Applicant/Assignee:
NTRU CRYPTOSYSTEMS INC, 5 Burlington Woods, Burlington, MA 01803, US, US (Residence), US (Nationality)
Inventor(s):
HOFFSTEIN Jeffrey, 3 Leicester Way, Pawtucket, RI 02860, US,
HOWGRAVE-GRAHAM Nicholas A, 30 Park Street, Arlington, MA 02474, US,
PIPHER Jill C, 3 Leicester Way, Pawtucket, RI 02860, US,
SILVERMAN Joseph H, 57 North Hill Avenue, Needham, MA 02492, US,
WHYTE William J, 20 Bay State Road, Somerville, MA 02144, US,
Legal Representative:
BEVILACQUA Michael J (et al) (agent), Hale and Dorr LLP, 60 State Street, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200350998 A1 20030619 (WO 0350998)
Application: WO 2002US38640 20021206 (PCT/WO US0238640)
Priority Application: US 2001338330 20011207
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 16591

Fulltext Availability:
Detailed Description

English Abstract
A method, system and apparatus for performing digital signatures and user identification. The signer's private key is a **short** generating **basis** for an NTRU **lattice** and his **public** **key** is a much longer generating bais for the same **lattice** . The signature on a digital document is a vector in the **lattice** with three important properties. - The signature is attached to the digital document being signed. - The signature demonstrates an ability to solve a general closest vector problem in the **lattice** . - The private vector of a general NTRU **lattice** is first used to construct a complete **short** **basis** for the **lattice** . Therefore, the RE is a straightforward linkage between the signature and the closest vector problem in the underlying NTRU **lattice** .

Detailed Description
... X = b for every value of b in S.

Another type of user identification technique relies on the difficulty of finding close vectors in a **lattice** . An identification technique of this type is described in Goldreich, S. Goldwasser, and S. Halevi, Public-key cryptography from lattice reduction problems, Proceedings of CRYPTO...The Verifier chooses a random vector (via a secure hash function) as the challenge.

The Prover uses the good almost orthogonal basis to find a **lattice** vector that is close to the challenge vector and sends this **lattice** vector to the Verifier. The Verifier accepts the Prover as securely identified if the response vector is in the **lattice** and is sufficiently

Springer-Verlag, 110
[17] A.J. Menezes and P.C. van Oorschot and S.A. Vanstone. Handbook ofApplied **Cryptography** , CRC Press, 1996.

[181 D. Micciancio, Improving **lattice** based **cryptosystems** using Hermite normalform, **Cryptography** and **Lattices** Conference-Proceedings of CaLC'01, (March 2001, Providence, RI), J. Silverman (ed.), Lecture Notes in Computer Science, Springer
Verlag, 126
[191 P. Nguyen, **Cryptanalysis** of the Goldreich-Goldwasser-Halevi **Cryptosystemfrom Crypto** '97, Advances in **Cryptology** -Proceedings of **CRYPTO** '99, (August 1519, 1999, Santa Barbara, California), M. Wiener (ed.), Lecture Notes in Computer Science, Springer-Verlag.
[201 T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes, Advances in **Cryptology - Crypto** '92, Lecture Notes in Computer Science 740 (E.F. Brickell, ed.)
Springer-Verlag, 1993, 31 [21] C.-P. Schnorr, A hierarchy ofpolynomial time **lattice** basis reduction algorithms,
Theoretical Computer Science 53 (1987), 201
[22] C.-P. Schnorr, A more efficient algorithmfor **lattice** basis reduction, J. Algorithms
9 (1988)@ 47
(23] C.-P. Schnorr. Efficient identification and signaturesfor smart cards, Advances in **Cryptology - Crypto** '89, Lecture Notes in Computer Science 435 (G. Brassard,
ed), Springer-Verlag, 1990, 239
[24] C.-P. Schnorr, M. Euchner, **Lattice** basis reduction: improved practical algorithms and solving subset sum problems, Math. Progranuning 66 (1994), no.

2, Ser. A, 181
(25] J. Stem. A new identification scheme based on syndrome decoding, Advances in **Cryptology - Crypto** '93, Lecture Notes in Computer Science 773 (D. Stinson, ed.),
Springer-Verlag, 1994, 13
[26] J. Stem. Designing

16/3,K/20 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01002148 **Image available**
MULTI-FACTOR AUTHENTICATION SYSTEM
SYSTEME D'AUTHENTIFICATION MULTIFACTORIELLE
Patent Applicant/Assignee:
WIRELESS KEY IDENTIFICATION SYSTEMS INC, d/b/a WiKID Systems, 817 W. Peachtree Street, Suite 205, Atlanta, GA 30308, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
OWEN William N, 1318 Fairview Road, Atlanta, GA 30306, US, US (Residence) , US (Nationality), (Designated only for: US)
SHOEMAKER Eric, 11640 Hauze Road, Roswell, GA 30076, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
TILLMAN Chad D (et al) (agent), Morris, Manning & Martin, L.L.P., 6000 Fairview Road, Suite 1125, Charlotte, NC 28210, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200332126 A2-A3 20030417 (WO 0332126)
Application: WO 2002US32403 20021009 (PCT/WO US0232403)
Priority Application: US 2001328310 20011009
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 19487

Fulltext Availability:
Detailed Description

Detailed Description
... approximately equivalent to RSAI 024 bits. The time for the key generation process averages 14 seconds.

The commercial embodiment uses the NTRU algorithm from NTRU **Cryptosystems** , Inc. for this key generation and in turn for the payload **encryption** . It is generally accepted that the **encryption** strength of the NTRU modified **lattice** algorithm is approximately the same as existing elliptical curve or RSA asymmetric algorithms. However, with the inferior computing power of wireless devices 922, the NTRU...

16/3,K/22 **(Item 6 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00875188 **Image available**
RING-BASED DIGITAL SIGNATURE AND AUTHENTICATION METHOD AND APPARATUS
SIGNATURE NUMERIQUE ET PROCEDE ET DISPOSITIF D'AUTHENTIFICATION
Patent Applicant/Assignee:
NTRU CRYPTOSYSTEMS INC, 5 Burlington Woods Drive, Burlington, MA 01803, US, US (Residence), US (Nationality)
Inventor(s):
HOFFSTEIN Jeffrey, 3 Leicester Way, Pawtucket, RI 02860, US,
PIPHER Jill, 3 Leicester Way, Pawtucket, RI 02860, US,
SILVERMAN Joseph H, 57 North Hill Avenue, Needham, MA 02492, US,
Legal Representative:
NEUNER George W (et al) (agent), Dike, Bronstein, Roberts & Cushman, Intellectual Property Practice Group, Edwards & Angell LLP, P.O. Box 9169, Boston, MA 02209, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200209348 A2-A3 20020131 (WO 0209348)
Application: WO 2001US23866 20010725 (PCT/WO US0123866)
Priority Application: US 2000220668 20000725; US 2001812917 20010320
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 17719

Fulltext Availability:
Detailed Description

Detailed Description
... illustrative embodiments. Alternative embodiments within. the scope of the appended claims will be readily apparent to those skilled in the art.

NSS: An NTRU **Lattice** -Based Signature Scheme
Jeffrey Hollstein, Jill Pipher, Joseph H. Silverman
NTRU Cryptosystems, Inc., 5 Burlington Woods, Burlington, MA 01803 USA, jhoff@ntru.com, jpipher@ntru...
...new authentication and digital si&nature scheme called the

of making Q larger does not continue indefinitely, and the ultimate result is to reduce the effective dimension of the lattice frem 2N...

...less randomly distributed in the interval [-q/2, q/2]. This yields 11,r1l Pz:: qVFN/-6 The vector -r is also contained in the **lattice** L p (p)2N ED . Let L.,, Lm n L. be the intersection. ...other words, letting IN denote the N-hy-N identity matrix and H the N-by-N circulant matrix formed from the coefficients of the **public key** h, the **lattice** L.,, is the intersection of the **lattices** generated by the rows of the fiollowing matrices.

H 0 0 0
Lm,p qINO n pIN () .

Mt 0 1
40
Then L.,, has determinant...feasible without the private key, and that it is not feasible to recover the private key from either a transcript of valid signatures or the **public key** .

42
We can, however, make a probabilistic argument for soundness under certain assumptions. For example, recall from Section 4.5 that the existence of a signed message (m, s) implies the existence of a vector in a **lattice** which (inverted exclamation mark)s a factor Of r. = Vr7@reg/(6p2) times larger than the expected smallest vector. We ha-ve chosen p @ 3...

...based on constmined polynomials, US Patent 6,076,163, June 13, 2000.

4. J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A new high speed **public key** cqffltosystem, in Algoriffimie Number Theory (ANTS 111), Portiand, OR, June 1998, Lecture Notes in Computer Science 1423 (3.P. BuhIer, ed.), Springer-Verlag, Berlin,
1998v 267
5. J. Hoffstein, J- Pipher, J.H. Silverman, NSS.- A Detailed Analysis of the NTRU **Lattice** -Based Signature Scheme, <www. ntrn. com>.

4 >
. J. Hoffstein, D. Lieman, J.H. Silverman, Polynomial Rings and Efficient **Public Key** Authentication, in Proceeding of the International Workshop on **Cryptographic** Techniques and E-Commerce (CrypTEC '99), Hong Kong, (M. Blum and C.H.

Lee, eds.), City University of Hong Kong Piess.

7. 3. Hoffstein, 3...

16/3,K/26 **(Item 10 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00843124
HYPERCOMPUTER
SUPERORDINATEUR
Patent Applicant/Assignee:
STAR BRIDGE SYSTEMS INC, 1192 East Draper Parkway, Mailstop 495, Draper, UT 84020, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
GILSON Kent, 928 East Rocky Mountain Lane, Draper, UT 84020, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
DURANT Stephen C (et al) (agent), Morrison & Foerster LLP, 755 Page Mill Road, Palo Alto, CA 94304-1018, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200175636 A2-A3 20011011 (WO 0175636)
Application: WO 2000US8772 20000515 (PCT/WO US0008772)
Priority Application: US 2000539318 20000330
Parent Application/Grant:
Related by Continuation to: US 2000539318 20000330 (CIP)
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK
EM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ
TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 16517

Fulltext Availability:
Detailed Description

Detailed Description
... is from the Gorin et al. patent, shows three PE boards 1., 2 and 3 with the port-to-port PE connections for a tree **lattice** structure. The PEs are shown not in their fixed **lattice** structure, but in the actual tree geometry for data flow, which can be created by configuring the PE ports. (Column 1 0, line 64-Colunm 1 1, line 9)
U.S. Patent No. 5,513,371 issued to **Cypher** et al., entitled HIERARCHICAL INTERCONNECTION NETWORK ARCHITECTURE FOR
3
PARALLEL PROCESSING, HAVING INTERCONNECTIONS BETWEEN BIT-ADDRESSABLE NODES BASED.ON ADDRESS BIT PERMUTATIONS, describes two new...

16/3,K/28 **(Item 12 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00828860 **Image available**
A DATA REPOSITORY AND METHOD FOR PROMOTING NETWORK STORAGE OF DATA
DEPOT DE DONNEES ET PROCEDE DE PROMOTION DE STOCKAGE RESEAU DE DONNEES
Patent Applicant/Assignee:
PERMABIT INC, 14 Portland Street, Cambridge, MA 02139, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
MARGOLUS Norman H, 4 Aldersey Street, #24, Somerville, MA 02143, US, US (Residence), CA (Nationality), (Designated only for: US)
KNIGHT Thomas F Jr, 58 Douglas Road, Belmont, MA 02178, US, US (Residence), US (Nationality), (Designated only for: US)
BOGHOSIAN Bruce M, 6134 Lexington Ridge Road, Lexington, MA 02421, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
LEE G Roger (agent), Fish and Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200161438 A2-A3 20010823 (WO 0161438)
Application: WO 2001US5355 20010220 (PCT/WO US0105355)
Priority Application: US 2000183466 20000218
Parent Application/Grant:
Related by Continuation to: US 2000183466 20000218 (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 24549

Fulltext Availability:
Detailed Description

Detailed Description
... since the dynamics is local and uniforin (see N.

Margolus, "A mechanism for efficient data access and communication in parallel computations on an emulated spatial **lattice** ," USPTO patent application, filed August 12, 1999). This is illustrated in Figure 1 1. In this example, the bit-string 90 to be **encrypted** can be taken to be the cell data for an n-dimensional CA space, with a plurality of bits associated with each cell. In the...

16/3,K/29 **(Item 13 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00800161 **Image available**
METHOD AND APPARATUS FOR DATA ENCRYPTION/DECRYPTION USING A DYNAMICAL SYSTEM
PROCEDE ET APPAREIL PERMETTANT DE CHIFFRER/DECHIFFRER DES DONNEES AU MOYEN D'UN SYSTEME DYNAMIQUE
Patent Applicant/Assignee:
QUIKCAT COM INC, Suite 200, 6700 Beta Drive, Mayfield Village, OH 44143, US, US (Residence), US (Nationality)
Inventor(s):
LAFE Olurinde E, 11795 Sherwood Trail, Chesterland, OH 44026, US,
Legal Representative:
JAFFE Michael A (agent), Arter & Hadden LLP, 1100 Huntington Building, 925 Euclid Avenue, Cleveland, OH 44115, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200133767 A2-A3 20010510 (WO 0133767)
Application: WO 2000US41864 20001103 (PCT/WO US0041864)
Priority Application: US 99435536 19991105
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7535

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... a fixed number of time steps Tf, where Tf = To + Td and 0 < To < Tf.

For symmetric encryption, the same rule set is used for **encryption** and **decryption** , whereas for non-symmetric **encryption** a different rule set is used to evolve the 3o dynamical system from time step To to time step T, .

Cellular Automata (CA) are dynamical systems in which space and time are discrete. The cells are arranged in the form of a regular **lattice** structure and must each have a finite number of states, wherein the state of each cell is typically criven by the Boolean variable a. These...

system, **lattice** size N, and boundary conditions.

26 A system according to claim 18, wherein said system further comprises **decryption** means for **decrypting** the **cyphertext** by further evolving the **cyphertext** in the dynamical system with a second dynamical rule set with preselected coefficients for Td time steps, wherein said data message is recovered at Tf...

16/3,K/30 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00777922 **Image available**
PRIVACY PRESERVING NEGOTIATION AND COMPUTATION
NEGOCIATION ET CALCUL PERMETTANT DE PROTEGER LA CONFIDENTIALITE
Patent Applicant/Assignee:
YEDA RESEARCH AND DEVELOPMENT CO LTD AT THE WEIZMANN INSTITUTE OF SCIENCE , P.O. Box 95, 76100 Rehovot, IL, IL (Residence), IL (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NAOR Simeon, 5 Beit Zuri Street, 69122 Tel Aviv, IL, IL (Residence), IL (Nationality), (Designated only for: US)
PINKAS Binyamin, 6 Eibeshiz Street, 62741 Tel Aviv, IL, IL (Residence), IL (Nationality), (Designated only for: US)
Legal Representative:
REINHOLD COHN AND PARTNERS (agent), P.O. Box 4060, 61040 Tel-Aviv, IL,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200111448 A2 20010215 (WO 0111448)
Application: WO 2000IL479 20000807 (PCT/WO IL0000479)
Priority Application: US 99148047 19990810; US 99428695 19991028
Designated States: IL JP US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 14323

Fulltext Availability:
Detailed Description

Detailed Description
... Hellman assumption (both the search and the decision problems, wherein the latter yields more efficient constructions), and the hardness of finding short vectors in a **lattice** (the Ajtai-Dwork **cryptosystem**). On the other hand, it seems to be highly unlikely that Oblivious Transfer can be based on one-way functions.

Following are the details of...

16/3,K/31 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00767969 **Image available**
SECURE USER IDENTIFICATION BASED ON RING HOMOMORPHISMS
IDENTIFICATION SURE D'UTILISATEUR SUR LA BASE D'HOMOMORPHISMES EN ANNEAU
Patent Applicant/Assignee:
NTRU CRYPTOSYSTEMS INC, 5 Burlington Woods, Burlington, MA 01803, US, US (Residence), US (Nationality)
Inventor(s):
HOFFSTEIN Jeffrey, 3 Leicester Way, Pawtucket, RI 02860, US,
SILVERMAN Joseph H, 57 North Hill Avenue, Needham, MA 02192, US,
LIEMAN Daniel, 32 Albany Drive, Colombia, MO 65201, US,
Legal Representative:
NOVACK Martin (agent), Building 1, 1960 Bronson Road, Fairfield, CT 06430 , US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200101625 A1 20010104 (WO 0101625)
Application: WO 2000US12025 20000503 (PCT/WO US0012025)
Priority Application: US 99132199 19990503
Designated States: AU CA CN IL JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 31366

Fulltext Availability:
Detailed Description
Claims

Detailed Description

... 503, 1n this paper we propose an approach to authenticaJ.

tion and digital signaturoR which is different from the square of the dimension of the **lattice** . (The same is traditional approach, but. is perhaps better suited for true or the **lattice** -based **cryptosystems** proposed in [1) applications involving low powered processors such as and [31.) In contrast, the keys used by NTRU and by smart cards and the authentication or certification of PASS, the authentication scheme in this paper, grow millions of micro transactions. The **public keys** we pro- only linearly with the dimension of the lattice, so they pose will be at least as secure from attack as RSA 1024 remain very practical even for **lattices** of dimension bebit keys. To kmsp the tratiscripts at a similar security tween 500 and 1000.

level, we will require. that the transcript lengths be re- More generally, the reason for re-examining the use of stricted to about 500. (This is a very conservative esti- lattice based **cryptosysterns** has to do with some of the mate.) However the case and speed of key pair genera- apparently fundamental limitations of **lattice** reduction tion will make it easy to leverage this, by a short tree of attacks and the nature of the **cryptosystems** that were validations, to millions of transactions d". cended from asuccessfully attacked in the past. In the most general simple key. terms, the LLL method, or its various improvements, As mentioned above., the hard problem underlying the will find a relatively short vector in a **lattice** L of dimensecurity of the **public key** in our scheme is related to Rion n in a surprisingly small amount of time. But one properties or short polynomials. Since short polyno- can ...

...analysis of these or the probabilistic expected length of the shortest vecschemes carefully consider the possibility of attack by tor if L were a random **lattice** . What seema to happen is **lattice** reduction methods. **Lattice** reduction attacks are that a first approximation by LLL or its improvements the general nanic for techniques ror finding short vectors will find a reasonably short vector in a **lattice** of dimenin **lattices** . The use or **lattice** attacks in **cryptography** sion n in time which grows polynornially in n. Further was pioneered by Sharnir,[171, who used it to break the refinements of LLL will find successively shortes vectors original knapsack based ptiblic key **cryptosystem** pro- with lengths that are still greater than the actual or exposed by (121. In the mid 80's Lmistra, Lenstra and Lo- pected shortest...

...Ultimately, LLL will always find vasz (91 introduced what hws since been called the LLL a vector either with the actual shortest length, or at **lattice** reduction method. This, mid further improve- any rate with length very close to the expected smallments on LLL by Schnorr, Eucliner and others [14, 15] est. However, the time required to find this vector seems led eventually to the breaking of all known **cryptosys** - to grow exponentially, or even super exponentially, with tems based on the difficulty of finding small vectors in the dimension n. We can summarize this in the following **lattices** . This includes the recent system proposed by very rough conjecture.

Aitai and Dwork [1) and by Goldreich, Goldwasser, and Conjecture I (Hard

equivalence. In Proc. basis reduction, J. Algorithms 9 (1988), 47 29th ACM Symposium an Theory of Computing, [16] C.-P. Schnorr. Efficient identification and signatures
1997,284 for smart cards. In G. Brassard, editor, Advances in
I-10
Cryptologo - O-Upto '89, I".ture Notes in Corn- commitment and the message and mapping the re
.4
puter Science 435, Springer-Wrlag (1990) 239 suit...

...g(S), g'(S), h). on perinuteil kernels. In G. Brassard, editor, Ad- aTo verify that Pearl signed the message Al, Vinnic vanccs in Cryptolek9y **Crypto** '89, Lecture Notes computes c from g(S),g'(S) and M, and then uses in Computer Science 435, Springer-Verlag (1990) Pearl's **public key** f (S) to verify that the response
606 h was generated by someone with knowledge of the
[191 J.H. Silverman, Dirriension-R.educed **Lattices** , Zero- private key f) f', i.e., by Pearl.
Forced **Lattices**

, and the NTRU **Public Key Cryptosystem** , NTRU Terlinical Note 013, March 2, The fundamental difference between the use of the
1999,(vvw.ntru.com) scheme for authentication and for digital signatures ...recover f.) In this section we will discuss and quatitify the difficulty of these questions. First we will discuss an attack on f using the **public key** I -f ((0 I ,,, ,
(section)2 Forniulation of a **lattice** attack on the **public key** . This is approached exactly as in 131. For convenience we will remind the reader of the outline. We begin by constructing a **lattice** as follows. For any polynomial F E R, associate to F the vector of coefficients (aolail ... aN-I)- Similarly for any such vector or point...public key system," Procee(lings or ANTS Ill, Portland (1998), Springer-Verlag. 131 J. 1 lofrst,cin, 1). Lictnan, J. Silverman, "Polynomial Rings and Efficient **Public Key** Autheritica-tion," Procccdhifj Qf the International Workshop on **Cryptographic** Techniques and E-Conaricrce (CrypTEC '99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press, to -rippear.
141 A. Nlay, Crypt.,malysis of NTRU, preprint, February 1999
[51 111. Silverman, Dimumioti-Reduced **Lattices** , Zero-Forced **Lattices** , and the NTRU **Public Key Cryptosystern** , NTRU Technical Note 013, March 2, 1999, (www. ntru. com)
Appendix 1. Timing Comparisons
In this sect-ioti we compare digital signature and verification times for various **cryptosysterns** . We note thal, the PASS2 times are based on a preliminary non-optimized implementation by Tao Groiip, Inc. We also note that the extremely fast...

16/3,K/32 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00766297 **Image available**
METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY
PROCEDE DE TRANSMISSION D'INFORMATION BINAIRE EN TOUTE SECURITE
Patent Applicant/Inventor:
KIM Donggyun, Korea University, Anam-dong 5-1, Seongbuk-gu, Seoul 136-701 , KR, KR (Residence), KR (Nationality)
BAE Jaegug, Dongsam-1dong, Youngdo-gu, Pusan 606-081, KR, KR (Residence), KR (Nationality), (Designated only for: US)
Legal Representative:
PARK Hae-sun, Yoksam-dong 824-19, Gangnam-gu, Seoul 135-080, KR
Patent and Priority Information (Country, Number, Date):
Patent: WO 200079692 A1 20001228 (WO 0079692)
Application: WO 2000KR640 20000617 (PCT/WO KR0000640)
Priority Application: KR 9922638 19990617
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KZ LC

LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI
SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: Korean
Fulltext Word Count: 5500

Fulltext Availability:
Claims

Claim
... that a problem information data is
easily leaked has occurred. Most of such attach methods rely
upon a low density attack method based on the **Lattice Basis**
Reduction Algorithm. A **small** number of the **public key**
transmission systems of the knapsack problem so far, including
one based on Chor-Rivest, are known to be safe against such
attach methods.
SUMMARY OF THE INVENTION
it is an object of the present invention to provide a
public key transmission system of an improved knapsack type for
securing higher safety by increasing transmission efficiency by
easily producing an public key and hardly extracting a...

16/3,K/33 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00576295 **Image available**
A METHOD FOR ACCELERATING CRYPTOGRAPHIC OPERATIONS ON ELLIPTIC CURVES
PROCEDE D'ACCELERATION DES OPERATIONS CRYPTOGRAPHIQUES SUR DES COURBES ELLIPTIQUES
Patent Applicant/Assignee:
CERTICOM CORP,
GALLANT Robert,
LAMBERT Robert J,
VANSTONE Scott A,
Inventor(s):
GALLANT Robert,
LAMBERT Robert J,
VANSTONE Scott A,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200039668 A1 20000706 (WO 0039668)
Application: WO 99CA1222 19991223 (PCT/WO CA9901222)
Priority Application: CA 2257008 19981224
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT
UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ
MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ
CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 7009

Fulltext Availability:
Detailed Description

Detailed Description
... of achieving this solution is described below in greater detail.

To produce small ai and bi, it is possible to make use of the L3-
lattice basis reduction algorithm (HAC p. 1 18), which would directly
result in **short basis** vectors. However, in this preferred embodiment
the simple extended Euclidean algorithm is employed on the pair (n, k).

The extended Euclidean algorithm on (n, k...

16/3,K/34 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00562056
A METHOD OF COMPRESSING DATA AND COMPRESSIBLE DEVICES
PROCEDE DE COMPRESSION DE DONNEES ET DISPOSITIFS COMPRESSIBLES
Patent Applicant/Assignee:
ORME Gregory Michael,
Inventor(s):
ORME Gregory Michael,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200025429 A1 20000504 (WO 0025429)
Application: WO 99AU913 19991021 (PCT/WO AU9900913)
Priority Application: AU 986660 19981022; AU 999781 19990416; AU 993360 19991012
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 12657
Fulltext Availability:
Detailed Description

Detailed Description
... the process as many times as desired. The key might contain parameters f or the shuf f ling algorithm as well as for decoding.

The **encryption** step might utilise for example available techniques such as DES or BLOWFISH.

To f acilitate the compression it may be desirable to structure the number in other forms to give more patterns, For example one might structure the number as a 2D or 3D **lattice** , or a **lattice** or

16/3,K/35 (Item 19 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00478148
METHOD AND DATA SYSTEM FOR DETERMINING FINANCIAL INSTRUMENTS FOR USE IN THE FUNDING OF A LOAN
PROCEDE ET SYSTEME DE DONNEES DESTINES A DETERMINER LES INSTRUMENTS FINANCIERS UTILISES DANS LE FINANCEMENT D'UN PRET
Patent Applicant/Assignee:
REALKREDIT DANMARK A S,
KRISTIANSEN Klaus,
BORGERSEN Borger,
LARSEN Bjarne Graven,
ROSENKRANS Mads,
LINDAHL Thomas,
TORNES-HANSEN Stig,
PETERSEN Bo Godthjaelp,
Inventor(s):
KRISTIANSEN Klaus,
BORGERSEN Borger,
LARSEN Bjarne Graven,
ROSENKRANS Mads,
LINDAHL Thomas,

TORNES-HANSEN Stig,
PETERSEN Bo Godthjaelp,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9909500 A2 19990225
Application: WO 98DK339 19980731 (PCT/WO DK9800339)
Priority Application: DK 090397 19970801
Designated States: AL AM AT AT AU AZ BA BB BG BR BY CA CH CN CU CZ CZ DE DE
DK DK EE EE ES FI FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK
LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK SL
TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG
KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF
BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 64236

Fulltext Availability:
Detailed Description

Detailed Description
... may be differentiated.

Further, the future zero-coupon rates are seen to depend on p which is the instant interest rate, whereas r in the **lattice** is a At period interest rate. However, a conversion from r to p is possible by means of (1.51). (1.51) provides the possibility of calculating a **longer** interest rate on the **basis** of a **short** -term interest rate. Let (t,T) be given by (t,t+At).

(1.55) P(tj t+At)=A(t, t+At)e -B(t...

16/3,K/36 (Item 20 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00430260 **Image available**
HIGH BANDWIDTH BROADCAST SYSTEM HAVING LOCALIZED MULTICAST ACCESS TO BROADCAST CONTENT
SYSTEME DE DIFFUSION EN LARGEUR DE BANDE ELEVEE DONNANT A LA DIFFUSION MULTIDESTINATAIRE UN ACCES LOCALISE AU CONTENU DE LA DIFFUSION
Patent Applicant/Assignee:
STARGUIDE DIGITAL NETWORKS,
Inventor(s):
DONAHUE Paul W,
DANKWORTH Jeffrey A,
HINDERKS Larry W,
FISH Laurence A,
LERNER Ian A,
BALLISTER Thomas C,
ROBERTS Roswell R III,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9820724 A2 19980522
Application: WO 97US20734 19971112 (PCT/WO US9720734)
Priority Application: US 9629427 19961112; US 9739672 19970228; US 9757857 19970902
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CZ DE DK EE ES FI
GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW
MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH
KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR
GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 31639

Fulltext Availability:
Detailed Description

Detailed Description
... supplied to the input of a descrambler 560 that decrypts the data in

conformance to the manner in which the data was, if at all, **encrypted** at the transmission site.

The embodiment of a descrambler 560 is illustrated in FIG. 19. In the illustrated embodiment, the descrambler 560 may be implemented by a field programmable gate array. One type of field programmable gate array technology suitable for this use is a **Lattice** isp 10 1 6.

The descrambler 560 preferably automatically synchronizes to the start of a DVB frame marker provided by the demodulator 555. The descrambler...

16/3,K/37 (Item 21 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00421267 **Image available**
METHOD, APPARATUS AND SYSTEM FOR COMPRESSING DATA
PROCEDE, APPAREIL ET SYSTEME DE COMPRESSION DE DONNEES
Patent Applicant/Assignee:
WDE INC,
ZADOR Andrew Michael,
Inventor(s):
ZADOR Andrew Michael,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9811728 A1 19980319
Application: WO 97CA452 19970625 (PCT/WO CA9700452)
Priority Application: US 96668753 19960624
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN GH KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 20302

Fulltext Availability:
Detailed Description

Detailed Description
... to the receiver, symbols embedded in the zerotree, and we can stop at a particular entropy, only transmitting the most significant ones.

5) If a **lattice** is used then there are ways to eliminate the codebook, thereby reducing image entropy. Another advantage is that if one does not use a codebook then one cannot **scramble** the image by losing or corrupting the codebook during transmission. (An error in the codebook spreads to all vectors sharing that codebook pointer, not just one vector in the image.) While a **lattice** vector quantizer is fast, it causes dents in images because objects near the center of a coarse Voronoi region round randomly based upon their truncated...

16/3,K/39 (Item 23 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00417862 **Image available**
PUBLIC KEY CRYPTOSYSTEM METHOD AND APPARATUS
PROCEDE ET APPAREIL RELATIFS A UN SYSTEME CRYPTOGRAPHIQUE A CLE REVELEE
Patent Applicant/Assignee:
NTRU CRYPTOSYSTEMS INC,
Inventor(s):
HOFFSTEIN Jeffrey,
PIPHER Jill,
SILVERMAN Joseph H,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9808323 A1 19980226

Application: WO 97US15826 19970819 (PCT/WO US9715826)
Priority Application: US 9624133 19960819
Designated States: AU CA CN IL JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 16886

Fulltext Availability:
Detailed Description
Detailed Description
... N'
operations to encode or decode a message consisting of N bits.

A fourth type of trap-door function which has been used to create **public key cryptosystems** is based on the knapsack, or subset sum, problem. These functions use a semigroup, normally the semigroup of positive integers under addition.

Many **public key cryptosystems** of this type have been broken using **lattice** reduction techniques, so they are no longer considered secure systems.

A fifth type of trap-door function which has been used to
SUBSTITUTE SHEET (RULE 26)
create **public key cryptosystems** is based on error correcting codes, especially Goppa codes. These **cryptosystems** use linear algebra over a finite field, generally the field with two elements. There are linear algebra attacks on these cryptosystems, so the key for a secure **cryptosystem** is a large rectangular matrix, on the order of 400,000 bits. This is too large for most applications.
A sixth type of trap-door function which has been used to create **public key** cryptcsystems is based on the difficulty of finding extremely **short** basis vectors in a **lattice** of **large** dimension N. The keys for such a system have length on the order of N2 bits, which is too large for many applications. In addition, these **lattice** reduction **public key cryptosystems** are very new, so their security has not yet been fully analyzed.

Most users, therefore, would find it desirable to have a **public key cryptosystem** which combines relatively short, easily created keys with relatively high speed encoding and decoding processes.

It is among the objects of the invention to provide...

...modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on elementary probability theory. The security of the **public key cryptosystem** hereof comes from the interaction of the polynomial mixing system with the independence of reduction modulo p and q. Security also relies on the experimentally observed fact that for most **lattices** , it is very difficult to find the shortest vector if there are a large number of vectors which are only moderately longer than the shortest...1 having N
ordered coefficients, some of which may be zero), and that the processor will perform designated operations on coefficients.]
The security of the **public key cryptosystem** hereof comes from the interaction of the polynomial mixing system with the independence of reduction modulo p and q. Security also relies on the experimentally observed fact that for most **lattices** , it is very difficult to find the shortest vector if there are a large number
of vectors which are only moderately longer than the shortest vector.

The **cryptosystem** hereof fits into the general framework of a probabilistic **cryptosystem** as described in M. Blum et

public key cryptosystems , Communications of the ACM 21 (1978), 120
11. C.P. Schnorr, Block reduced **lattice** bases and successive minima, Combinatorics,
Probability and Computing 3 (1994), 507
12. C.P. Schnorr, H.H. Hoerner, Attacking the Chor Rivest Mptosystem by improved **lattice** reduction. Proc. EUROCRYPT 1995, Lecture Notes in Computer Science
921, Springer-Verlag, 1995, pp. 1
13. D. Stinson, **Cryptography** : Theory and Practice, CRC Press, Boca Raton, 1995.

16/3,K/40 (Item 24 from file: 349)

00383956 **Image available**
AUTHENTICATION OF ARTICLES
AUTHENTIFICATION D'ARTICLES
Patent Applicant/Assignee:
S E AXIS LIMITED,
KARIAKIN Youry D,
Inventor(s):
KARIAKIN Youry D,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9724699 A1 19970710
Application: WO 95GB3051 19951229 (PCT/WO GB9503051)
Priority Application: WO 95GB3051 19951229
Designated States: AU BB BG BR CA CN CZ EE FI HU IS JP KR KZ LK LT LV MD MX NO NZ PL RO TT UA UG US VN AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 9382

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... circular dichroism spectrum, spectrum of anomalous dispersion of x-rays, individual combinative dispersion spectrum,'gas electronography, oscillatory infrared, electronic or ultraviolet spectrum, the crystalline or **lattice** structure of the material constituting the article.

Preferably the encoded characteristic is **encrypted** and **decrypted** using a **public key encryption** system and advantageously the **public key encryption** system has a plurality of levels of security.

Preferably means are also provided for encoding additional characterising information together with the representation of the physical...

Claim
... circular dichroism spectrum, spectrum of anomalous dispersion of x-rays, individual combinative dispersion spectrum, gas electronography, oscillatory infrared, electronic or ultraviolet spectrum, the crystalline or **lattice** structure of material constituting the article.

14 A method of authenticating articles as claimed in any of the preceding claims wherein the encoding is **encrypted** and **decrypted** using a **public key encryption**

15 A method of authenticating articles as claimed in claim 14 wherein the **public key encryption** system has a plurality of levels of security.

16 A method of authenticating articles as in any of the preceding claims wherein additional characterising information...

16/3,K/42 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00364089 **Image available**
AN ELECTRONIC MICRO IDENTIFICATION CIRCUIT THAT IS INHERENTLY BONDED TO A SOMEONE OR SOMETHING
CIRCUIT DE MICRO-IDENTIFICATION ELECTRONIQUE INHERENT A QUELQU'UN OU A QUELQUE CHOSE
Patent Applicant/Assignee:
DALLAS SEMICONDUCTOR CORPORATION,
Inventor(s):
BOLAN Michael L,
FEKETE Nicholas,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9704414 A2 19970206
Application: WO 96US11882 19960719 (PCT/WO US9611882)
Priority Application: US 951303 19950720
Designated States: AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 2743
Fulltext Availability:
Detailed Description

Detailed Description
... of physical and electronic barriers. Such barriers include, but are not limited to 1) having 4 temperature window of operation; 2) interlaced power and ground **lattice** ; 3) solder bump/flip-chip technologies; 4) module tampering alarm circuitry; 5) SRAM destruction circuitry on tampering of the electronic module; 6) RSA **encryption** capabilities for bidirectional communication. Thus, the electronic module is extremely difficult to copy, counterfeit, or to **decipher** its communications.